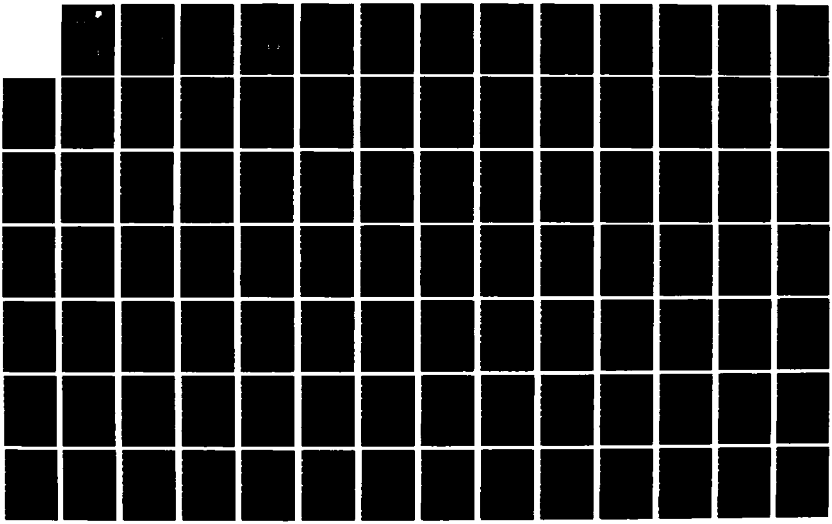
AD-A147 922 HYBRID TECHNIQUES INVESTIGATION(U) SHANE-GELLING CO SEA 1/3
CLIFF NY D C SHANE ET AL. APR 84 SGR-84-01
RADC-TR-84-60 F30602-82-C-0167

UNCLASSIFIED F/G 17/2 NL



(12)

RADC-TR-84-60
Final Technical Report
April 1984

HYBRID TECHNIQUES INVESTIGATION

Shane-Gelling Company

Dale C. Shane, Scott C. Shane, Michael E. Nowak and Donna M. Fare

Sponsored by
Defense NuclearAgency

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

ROME AIR DEVELOPMENT CENTER
Air Force Systems Command
Griffiss Air Force Base, NY 13441

This report has been reviewed by the RADC Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RADC-TR-84-60 has been reviewed and is approved for publication.

APPROVED: Melvin G. Manor, Jr.

MELVIN G. MANOR, Jr.
Project Engineer

APPROVED: Albert A. Jamberdino

ALBERT A. JAMBERDINO
Acting Technical Director
Intelligence & Reconnaissance Division

FOR THE COMMANDER: John A. Ritz

JOHN A. RITZ
Acting Chief, Plans Office

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS N/A
2a. SECURITY CLASSIFICATION AUTHORITY N/A 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
4. PERFORMING ORGANIZATION REPORT NUMBER(S) SGR-84-01	5. MONITORING ORGANIZATION REPORT NUMBER(S) RADC-TR-84-60
6a. NAME OF PERFORMING ORGANIZATION Shane-Gelling Company 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION Rome Air Development Center (IRAA)
6c. ADDRESS (City, State and ZIP Code) 324 Littleworth Lane Sea Cliff NY 11579	7b. ADDRESS (City, State and ZIP Code) Griffiss AFB NY 13441
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Defense Nuclear Agency 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER F30602-82-C-0167
8c. ADDRESS (City, State and ZIP Code) Wash DC 20305	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO.: 62715H PROJECT NO.: DNAR TASK NO.: 02 WORK UNIT NO.: 37
11. TITLE (Include Security Classification) HYBRID TECHNIQUES INVESTIGATION	

12. PERSONAL AUTHOR(S)
Dale C. Shane, Scott C. Shane, Michael E. Nowak, Donna M. Fare

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Yr., Mo., Day)	15. PAGE COUNT
Final	FROM Nov 82 TO Nov 83	April 1984	208

16. SUPPLEMENTARY NOTATION
Sponsored by the Defense Nuclear Agency

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB. GR.	
09	03		Hybrid System Personal Identity Verification Entry Control
12	02		

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

A Hybrid Techniques Investigation has been undertaken wherein a design of an electronic interface unit has been considered, capable of linking multiple Personal Identity Verifier (PIV) devices at an Entry Control Point with a Host computer. The Hybrid Interface Unit (HIU), acting as an element within an overall Entry Control System, controls the operation of the individual PIV's and other elements within the entry portal in response to orders from the host computer that certain levels of security be obtained as an operating condition for the portal and for the Base. The Hybrid Interface Unit selects the arrangement of, and the thresholds for, each of the PIV's as logical devices for each entrant in such a way that the full potential of the hybridization concept is realized, as identification errors are reduced and throughput is increased for the full range of the population.

In conjunction with the HIU design, an Entry Control System architecture in the Host has (Cont'd)

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Melvin G. Manor, Jr.	22b. TELEPHONE NUMBER (Include Area Code): (315) 330-3651 22c. OFFICE SYMBOL: RADC (IRAA)

DD FORM 1473, 83 APR — EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

been examined that utilizes distributed processing elements to meet the functional performance and timing requirements mandated by the hybrid design. The distributed processing within the Host is split among three individual functional groups, loosely joined with each other.

The Hybrid Interface Unit design, although it controls the operations within the portal directly, has been formulated to be a part of a feedback command/control loop including the analysis portion of the Enrollment Processor and the Security Command/control portion of the C3 Processor. The feedback allows the HIU's operating parameters to be controlled and upgraded over a selected time period, from the Host, as actual operating conditions become known in order to most readily apply the potential performance levels the hybridization concept is capable of providing.

In the formulated design resulting from the hybrid investigation, the HIU processes have been defined in an algorithm whose routines are held in an EPROM in the single board microprocessor which embodies the HIU. All data tables, PIV drivers, portal element drivers, communication drivers, command information and messages, as well as the HIU executive, are to be laid in either EPROM or RAM on the HIU board.

Operating characteristics required of, and available from the individual PIV's for proper operation within the Hybrid System have been defined as a result of a survey. Signal interface requirements have been identified and have been determined to be within the vendor's capability to supply, for those PIV's selected as suitable for use with the concept.

The Hybrid Performance Algorithm has been formulated, that relates analysis of collected data to actual system error performance over the entire Entry Control System, and computes the new parameters from the monitored data that permit the commanded security levels within the limits of hybrid performance to be achieved.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Figure		Page

LIST OF TABLES

SECTION 1

INTRODUCTION AND SUMMARY

A Hybrid Techniques Investigation has been undertaken wherein a design of an electronic interface unit has been considered, capable of linking multiple Personal Identity Verifier (PIV) devices at an Entry Control Point with a Host computer. The Hybrid Interface Unit (HIU), acting as an element within an overall Entry Control System, controls the operation of the individual PIV's and other elements within the entry portal in response to orders from the host computer that certain levels of security be obtained as an operating condition for the portal and for the Base. The Hybrid Interface Unit selects the arrangement of, and the thresholds for, each of the PIV's as logical devices for each entrant in such a way that the full potential of the hybridization concept is realized, as identification errors are reduced and throughput is increased for the full range of the population.

In conjunction with the HIU design, an Entry Control System architecture in the Host has been examined that utilizes distributed processing elements to meet the functional performance and timing requirements mandated by the hybrid design. The distributed processing within the Host is split among three individual functional groups, loosely joined with each other:

1. An IDENT Processor, functioning solely to respond rapidly to the requests from the reference files, in order to reduce queuing delays to a minimum.

2. A C3 processor, operating as the primary housekeeper, routing raw data from the portals, accepting and acting upon alarms, deciding the levels of security required for the Base, communicating with the Base Commander and with each Portal on all matters except reference file retrieval.

3. An Enrollment Processor, responsible for enrollment, that collects and stores archivals, prepares reference files to present to the IDENT Processor, and performs analysis on raw data from each portal in near real-time in order to permit monitoring of achieved performance and to command new performance levels, in the operational environment.

The Hybrid Interface Unit design, although it controls the operations within the portal directly, has been formulated to be a part of a feedback command/control loop including the analysis portion of the Enrollment Processor and the Security Command/control portion of the C3 Processor. The feedback allows the HIU's operating parameters to be controlled and upgraded over a selected time period, from the Host, as actual operating conditions become known in order to most readily apply the potential performance levels the hybridization concept is capable of providing.

In the formulated design resulting from the hybrid investigation, the HIU processes have been defined in an algorithm whose routines are held in an EPROM in the single board microprocessor which embodies the HIU. All data tables, PIV

drivers, portal element drivers, communication drivers, command information and messages, as well as the HIU executive, are to be laid in either EPROM or RAM on the HIU board.

Operating characteristics required of, and available from the indivdual PIV's for proper operation within the Hybrid System have been defined as a result of a survey. Signal interface requirements have been identified and have been determined to be within the vendor's capability to supply, for those PIV's selected as suitable for use with the concept.

The Hybrid Performance Algorithm has been formulated, that relates analysis of collected data to actual system error performance over the entire Entry Control System, and computes the new parameters from the monitored data that permit the commanded security levels within the limits of hybrid performance to be achieved.

SECTION 2

THE HYBRID CONCEPT

Several types of Personal Identity Verifiers have been developed by industry for use in entry control systems. These devices have based the verification on some class of physical or behavioral characteristic that is amenable to being processed electronically and being placed in binary digital form as a reference set. However, each characteristic set, i.e., a voice pattern, palm geometry, a fingerprint pattern, has been developed as a device independently from the others. It seems reasonable that a Hybrid formed by combining a group of these PIV devices would permit a more positive identity verification, inasmuch as they measure at once a statistically larger set of physical or behavioral characteristic from the same person. A simulation has shown that considerable performance improvement can be obtained by combining two or more available entry control devices in some logical configuration of "AND"s and "OR"s.

As an example, if a person were required to verify on two separate device types, i.e., voice and fingerprint, to be allowed through an entry control portal operating in an "AND" configuration, the system Type I error would be additive of the individual errors and the system Type II error would be multiplicative. Under this configuration, system Type II error is considerably enhanced with little sacrifice to Type I error and throughput.

----

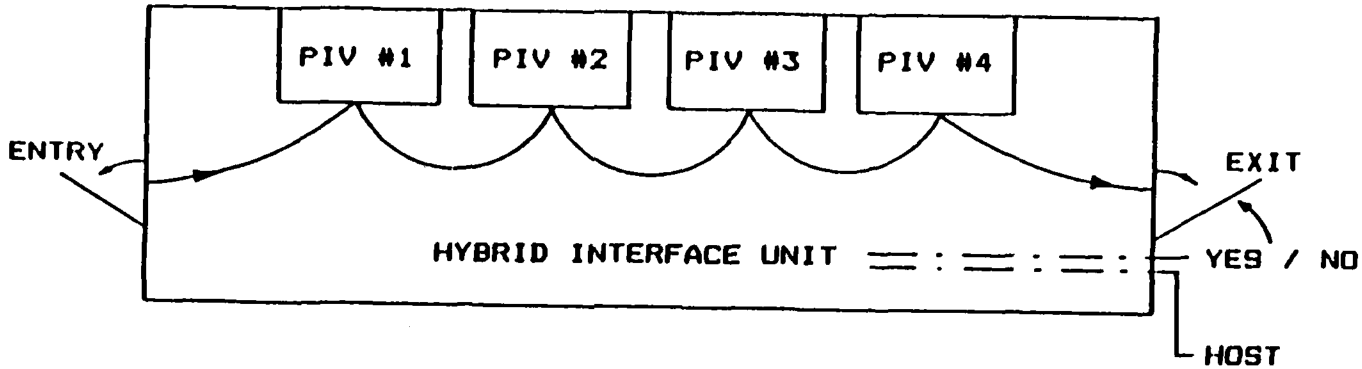
1. Harold Rosenbaum Associates, Entry Control System Analysis: Hybrid Control Study, RADC-TR-82-28, Vol. 1, March 1982.

Physically, a hybrid grouping is achieved by co-locating the different PIV's in an Entry Control Portal through which an entrant must pass in order to be admitted to the secure side. Electronically, the hybrid processing is accomplished in a Hybrid Interface Unit (HIU) also co-located in the portal, which accepts the match results from each PIV acting in turn, and combines the results in conformance with the logical dictates of the Hybrid Algorithm. This concept is shown in Figure 2-1. Some, or all, of the PIV's may be used by any entrant, depending upon the specific entry requirements determined to be in effect by the HIU.

Table 2-1 lists the different logical configurations available in a multi-PIV device Hybrid System. Each logical combination in AND and OR defines the PIV used and the method by which individual PIV error statistics are combined to produce an overall system error with that logical combination. Similar Tables can easily be established for four-or-five-device Hybrid Systems.

The hybrid concept has value also in aiding authorized entrants who may have difficulty with any particular PIV, by permitting the bypass of any particular PIV device, as long as overall system error requirements have been satisfied. This may be accomplished by commanding the HIU to select the logical configuration and the individual scoring thresholds that determine the entry decision requirements, in such a way that an "accept" decision is correctly made within the desired error limits using the minimum number of PIV's.

Persons having persistently poor scores on any PIV (e.g. a stutterer would have difficulty with a voice PIV) are herinafter called "goats." Test experience indicates that goats exist with



BEST COMBINATION	(1 OR 2) AND (3 OR 4)
BEST TYPE I / WORST TYPE II	1 OR 2 OR 3 OR 4
BEST TYPE II / WORST TYPE I	1 AND 2 AND 3 AND 4
MODERATES:	ANY OTHER COMBINATION

Figure 2-1: HYBRID ACTION IN THE PORTAL

Table 2-1

LEGITIMATE DEVICE CONFIGURATIONS
IN A HYBRID ENTRY CONTROL SYSTEM

DEVICE COMBINATION	SYSTEM ERRORS: ALPHA	BETA
S1 AND S2	$\alpha 1 + \alpha 2$	$\beta 1 * \beta 2$
S1 OR S2	$\alpha 1 * \alpha 2$	$\beta 1 + \beta 2$
S1 AND S2 AND S3	$\alpha 1 + \alpha 2 + \alpha 3$	$\beta 1 * \beta 2 * \beta 3$
S1 OR S2 OR S3	$\alpha 1 * \alpha 2 * \alpha 3$	$\beta 1 + \beta 2 + \beta 3$
(S1 AND S2) OR S3	$(\alpha 1 + \alpha 2) * \alpha 3$	$(\beta 1 * \beta 2) + \beta 3$
(S1 OR S2) AND S3	$(\alpha 1 * \alpha 2) + \alpha 3$	$(\beta 1 + \beta 2) * \beta 3$
(S1 AND S2) OR (S3 AND S4)	$(\alpha 1 + \alpha 2) * (\alpha 3 + \alpha 4)$	$(\beta 1 * \beta 2) + (\beta 3 * \beta 4)$

LEGEND:

Si Represents PIA Device i, (i=1, 2, 3, 4)

αi Represents Device Level Type I Error Probability

βi Represents Device Level Type II Error Probability

poor score distributions, although, for various reasons, test data does not as yet indicate the proportion of the population occupied by goats. Further, test data does not yet indicate whether a person who is a goat on one PIV device is also a goat on another PIV device. The independent nature of the feature sets of the PIV's would suggest, however, that a goat on one device is not a goat on another, except coincidentally, which coincidence would make their individual population percentages multiply. Attributing all of PIV error data to goats would indicate that goats exist among the population at an order-of-magnitude level of one percent depending on the definition used, and could be postulated at a level of five percent under certain conditions.

A Type I goat may be described as an entrant into the ECS system, who has difficulty matching his own reference file. A Type II goat may be described as an entrant whose reference file set is highly susceptible to being matched by many others in the population.

SECTION 3

PERSONAL IDENTITY VERIFIERS

A. GENERAL

The availability of Personal Identity Verification (PIV) device types, suitable for use as elements in the Hybrid System, has been established and is described in Table 3-1 for a number of the PIV types. These devices sense physical or behavioral features from an individual that are sufficiently independent to allow the statistical manipulation of "and-ing" and "or-ing" inherent in the hybrid grouping concept. Futhermore, the devices utilize technology that is sufficiently advanced, in the judgement of the authors, to justify their consideration as elements in an operational system for military use. Data contained in the accompanying table was obtained either directly from the device manufacturers or from a second source, i.e., brochures or prior reports. The table is intended to describe the PIV as a generic device, a device supportable by today's technology rather than a specific manufacturer's product. The study showed, among other things, that the technology is still moving ahead rapidly under the inducement of commercial market possibilities and that such parameters as form factors, sensor technique, processing speed, and error performance, are all advancing to and beyond the point of sufficiency for hybrid usage.

A comparison of the table with specific products should show that one or more manufacturers has attempted to market a PIV of each type that is very close to that described in the table, with differences primarily in form and fit, rather than performance. It can be expected that other PIV's will undergo development, and when available, can be added to the list, if they meet the following requirements associated with the Hybrid System:

Table 3-1
AVAILABLE PIV TECHNOLOGY (1 of 3)

CHARACTERISTIC	DEVICE #1	DEVICE #2	DEVICE #3
1) PIV DEVICE TECHNOLOGY	Hand Measurements	Finger Print	Retinal Pattern
2) CURRENT OPERATIONAL STATUS	Quantities Sold to Gov't Agencies	Development Quantities Manufactured	Development Quantities Manufactured
3) EXTENT OF TESTING PERFORMED	> 100 Persons	> 100 Persons	> 100 Persons
4) VALID TYPE II PERFORMANCE DEMONSTRATED	< 2% at 1% Type I	< 1% at 1% Type I	< 1% at 1% Type I
5) OPERATIONAL X-CURVES AVAILABLE	Yes	Yes	Yes
6) CORRELATABLE WITH OTHER PHYSICAL/ BEHAVIORAL CHARACTERISTICS	Essentially Independent	Essentially Independent	Essentially Independent
7) ENROLLMENT TIME PER USER	< 5 min.	< 5 min.	< 5 min.

AVAILABLE PIV TECHNOLOGY (2 of 3)			
CHARACTERISTIC	DEVICE #1	DEVICE #2	DEVICE #3
8) OPERATIONAL ENTRY TIME PER ATTEMPT	< 4 sec. Processing Time	< 4 sec. Processing Time	< 4 sec. Processing Time
9) AVERAGE NUMBER OF ATTEMPTS PER ENTRY	1+	1+	1+
10) REMOTE TERMINAL SEPARATE FROM HOST	Yes	Yes	Yes
11) INTERFACE TO HOST DEFINED	Yes	Yes	RS-232 IEEE-488
12) MATCH SCORE AVAILABLE TO HOST	Yes	Yes	Yes
13) MATCH THRESHOLD VARIABLE -- IN RAM	Can be Obtained	Can be Obtained	Can be Obtained
14) MATCH ALGORITHM AVAILABLE	Company Controlled	Company Controlled	Company Controlled
15) SIZE OF FILE -- IN HOST	< 100 Bytes	< 500 Bytes	< 500 Bytes
16) NUMBER OF BACKUP IMAGES IN HOST	None; One Available	More Than One Available	None; One Available
17) COMPLEXITY OF MATCH ALGORITHM (SCALE OF 10)	2	8	5

AVAILABLE PIV TECHNOLOGY (3 of 3)			
CHARACTERISTIC	DEVICE #1	DEVICE #2	DEVICE #3
18) MOST PROBABLE USER-UNFRIENDLY FEATURE	Fingernail Length Variations	Improper Finger Laydown	Eyelash Interference
19) DESIGN IMPROVEMENTS POSSIBLE	Yes -- More Features	Yes	Yes
20) AREA OF VULNERABILITY TO IMPOSTERS	False Hand Models	False Finger Models	False Eye Models
21) SUSCEPTIBILITY TO BACKGROUND/ AMBIENT INTERFERENCE	Avoid Bright Sources of Light	Avoid Heavy Vibration, Humidity	Avoid Heavy Vibration, Humidity
22) SIZE (in.) AND NUMBER OF SEPARATE PACKAGES	1. 13x21x20 2. Smaller	1. 15x15x20 2. Smaller 3. Smaller	1. 6x14x15
23) WEIGHT AND POWER REQUIREMENTS	< 45 lbs. < 1 KW	< 50 lbs. < 1 KW	< 20 lbs. < 1 KW
24) PROBABLE COST	est < $5K	est < $15K	est < $10K
25) SINGLE MOST COSTLY ELEMENT -- AND ITS COST	Scanner est < $2K	Scanner est < $5K	Scanner est < $4K

a) operate as a standalone device, i.e., extract features in real time and perform an internal match against reference features obtained from a host.

b) generate a match score representative of the degree of feature match or mismatch, and present the score to the host as a part of the transaction record.

c) temporarily buffer the raw feature set extracted in real time, and present the set to the host as a part of the transaction record.

d) use a feature set that is machine-extractable within a machine-measurement tolerance small compared to the expected feature variation among separate renditions from the same individual.

e) use a feature set that is homogenous across the population and consistently available to the machine, so that Type I/Type II error data can be processed on a regular basis.

f) use a feature set that has statistical properties within the set, and can be considered independent of the feature set contained in another PIV.

g) provide an error performance of one percent or better at crossover, on the basis of a single-set match.

h) perform the extraction and matching operations within a period of three seconds or less.

i) have a feature set whose size is less than 5K Bytes.

j) requires no file update except for occasional re-enrollment.

k) have a physical size and module form factor reasonably befitting space availability in a typical portal design.

l) have an elemental cost less than $15K.

Each PIV must produce a generic set of parameters,indicated in Figure 3-1, for use by the HIU, that fits the requirements of the Hybrid System interface. Included are the numerical score resulting from the match attempt, and the raw feature set, defined as the newly extracted set, with nuances, closely equivalent to the reference set. The score and the raw feature set are typically transmitted to the Hybrid Interface Unit as the equivalent of the PIV's Transaction Record. From the HIU, a standby/enable signal is available to the PIV in order to initiate the entry action and to inform the PIV that a reference file transfer is imminent.

Two parameters normally produced by the PIV, namely, the threshold level and the Accept/Reject decision signal, are not required when the PIV is operating as a Hybrid element.

It should be noted that PIV availability from Table 3-1 is considered positive even though some repackaging or software interface modifications may be required of the unit, and even

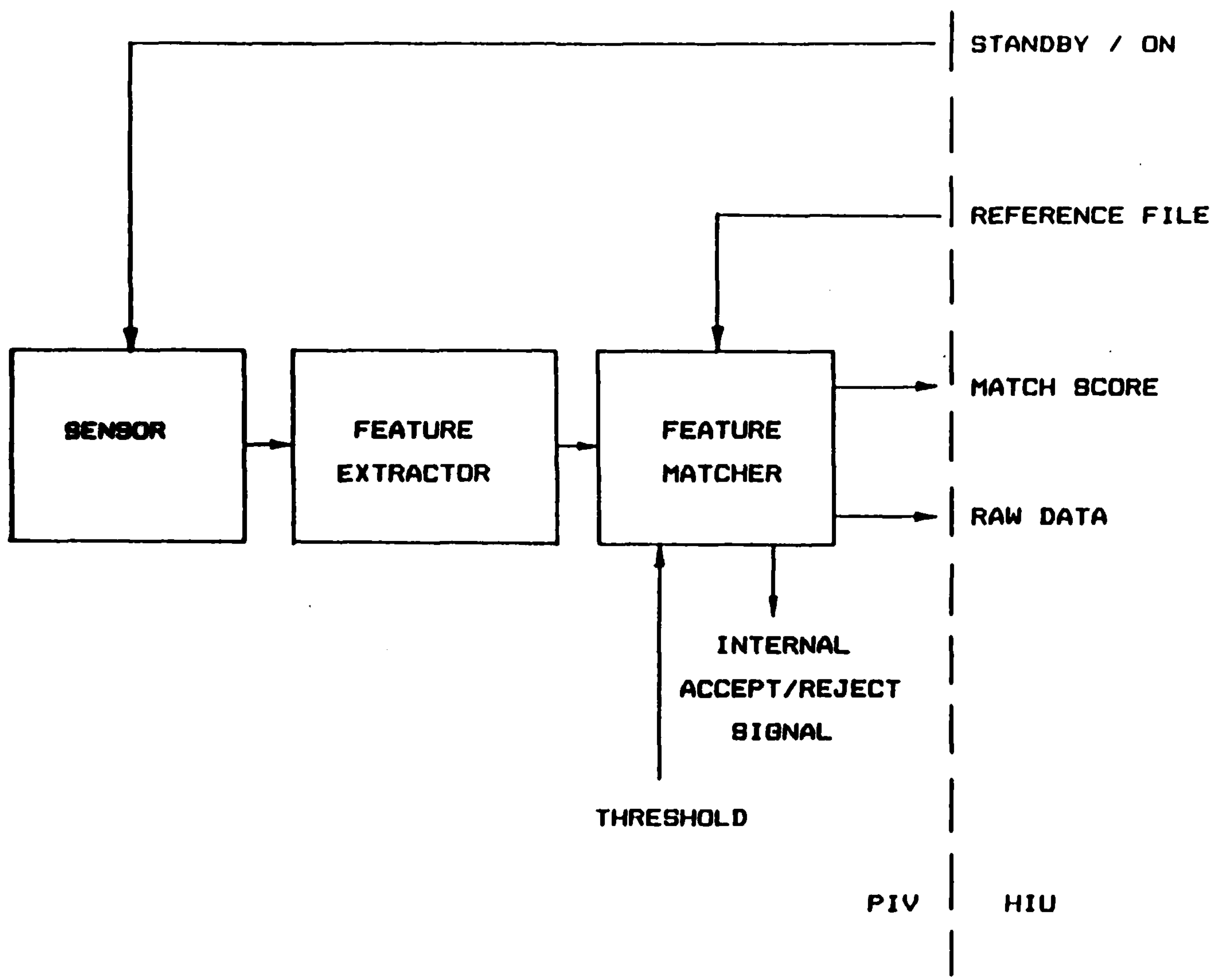


Figure 3-1: STANDALONE PIV FUNCTIONS DURING ENTRY

though thorough testing of error performance has not necessarily been achieved to date.

Discussions with manufacturers about documenting performance has revealed that sufficiently definitive data is not available, for the most part, to prove performance over the entire range of interest to the military. The data made available to date, with a few exceptions, has been limited to a trial-and-error collection process using statistically valid entries over a limited range, principally in support of the device development process. Each of the PIV device types has a predicted Type I/Type II error rate around 1.0 percent, although some data indicates that operation at a Type II rate of 0.1 percent in some devices is achievable when holding Type I at 1.0 percent. The ultimate limitations of each device type has not been explored to any great depth, with the exception of speaker identification (voice upgrade program).

B. TECHNOLOGY LIMITATIONS

Several factors are inherent with each device which tend to restrict performance in an operational environment. A speaker verification device type, for example, measures physical and behavioral features whose statistical characteristics become more recognizable, more consistent, with usage, experience, and time. The greater the amount of data extracted, the longer the speaking time over which the information is gathered, the greater the predictability that the behavioral characteristic "belongs" to any candidate for entry into the secure area. Further, as the candidate introduces more data, over a period of time, the statistics become more sharply defined, rounded out until a point of diminishing returns concerning performance is reached with respect to any given feature. Although the precision of the equipment doing the extraction and measurement of the set of

features has limitations, with today's state-of-the-art technology it is more likely to be the non-constancy of the feature itself, within the limited observation time, from rendition to rendition, that forces the reaching of the point of diminishing returns. Honing of the behavioral feature by the candidate, can be done, with practice, with experience. A reference file update on a per-try basis can also be accomplished in order to enable tracking the most recent set of statistics. A learned matching of the man to the machine to ever-increasing levels is possible. However, steps of this type become specifically counterproductive whenever a usage layoff of any duration (such as TDY or a long weekend) occurs. The learned match levels deteriorate, prior levels cannot be immediately repeated, and Type I error probability increases until a new learned level can be established, perhaps through a reenrollment. This operational limitation is better traded off against a backed-off performance level, especially for hybrid application.

C. POPULATION LIMITATIONS

Error improvements for the behavioral features, when at the point of diminishing returns, are rendered more difficult to achieve by the variation, by cross section of the population, in the inherent ability of the candidate to adapt to vagaries of the device. In the voice system, attempts at standardization of prompts, of utterances, in timing of utterances, etc., meet with resistance from some segment of the population at both ends of the spectrum. It is axiomatic that this would be true for any PIV using behavioral features; the very element that makes the characteristic so distinctive, its wide range across the population, places cutoffs on the amount of standardization achievable in the practical system, if the entire population is to be accommodated. Conversely, practical standardization in the machine and its concept, creates an isolation of some segment of

the population. In the area of behavioral features, if a casual Type II error rate is to be tested, some form of standardization is necessary if it is to be assured that applicable data is available in the reference file set, to monitor the proper comparison, i.e., that apples are compared to apples among the population.

D. PROCESSING LIMITATIONS

Processing time tradeoffs also lead to diminishing returns, in that excessive throughput penalites are incurred, if a high threshold (or learning level) is decreed that forces multiple retrials. Similarly, throughput is penalized if longer utterances (more phrases) are decreed that force excessive processing time.

In any PIV, the score derived from the comparison of any newly-derived feature set and the file reference set is desired to be consistently close in value to the nominal score, if standards are to be established that promote better Type I/Type II error performance. A low standard deviation about any individual's nominal score value might be expected on successive renditions if the newly-derived feature set was a consistent set. PIV's developed to date indicate nominals and standard deviations of the type shown in Figure 3-2 can be assumed. For the sake of description, the population has been postulated as occupying four groups. The majority of the population, curve C, fits within its own statistically-derived variance at some nominal score value. A portion of the population are super achievers, as in curve A, capable of adapting well to the machine's requirements, and having a feature set that is consistently repeatable. At the other extreme, a portion of the population are poor achievers, curve B, consistently unable to obtain a decent score for any number of reasons. Close by are the participants, curve D, who

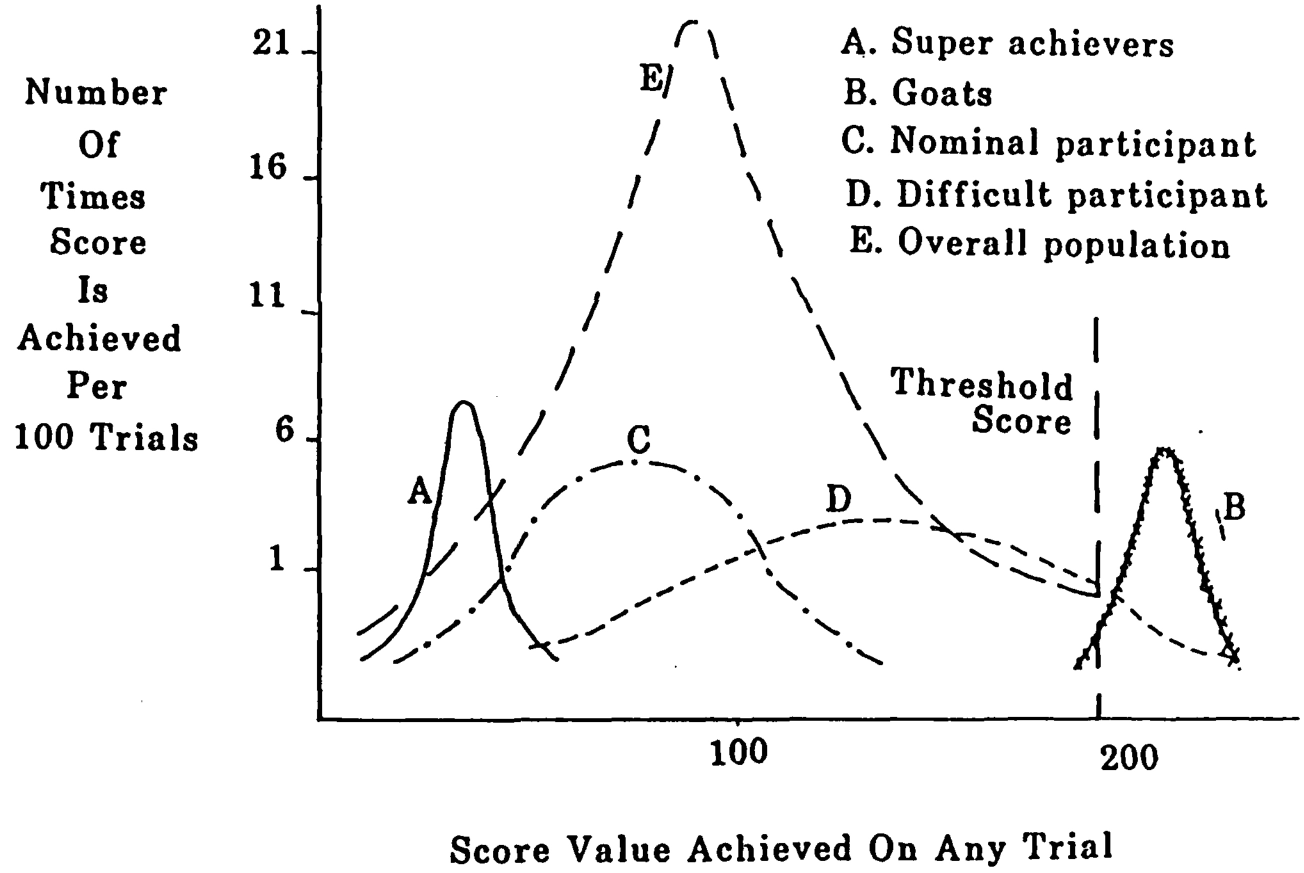


Figure 3-2: COMPARISON OF DIFFERENT USER DISTRIBUTIONS IN A TYPICAL POPULATION

have difficulty in getting repeatable scores, but are nevertheless able to adapt to the concept to some degree, while contributing to both Type I and Type II system errors.

When personal identity patterns are involved, it is not reasonable to expect perfectly matched patterns to recur. The "best fit" concept is an attempt to make up for the users inability to consistently reference his image pattern in the properly registered position, with respect to up-down and right-left directions, rotation, or magnifications. Pattern skewness is bound to cause a poor match score due either to insertion of false data or omission of true data. Other reasons for poor match scores are presented in Table 3-2.

Since image patterns with some degree of difference are inherent in PIV systems, a range of scores can be expected to occur over multiple match attempts. Threshold score can be defined as that score beyond which the match score cannot extend if the users identity is to be verified by that score. The threshold score is a statistically sound value, with which the amount of mismatch can be safely predicted between each users current file and his reference file that could result in an error in his identity verification. Typical score value distributions on any individual are shown in Figure 3-3.

An error in identity verification occurs if a true user is falsely rejected, defined as a Type I error, and if an imposter, a false user, is accepted, defined as a Type II error. Type I and Type II error curves are obtained empirically. A PIV device type has a Type I error, applicable to the entire population of its users, that measures how well the device can perform the identity verification in its operational performance on all users without error, obtained as a percentage number by dividing the quantity of false rejections by the total quantity of

TABLE 3-2

BASIS FOR POOR SCORES ON PIVs

1. HAND GEOMETRY

* Improper finger spread
* Fingernail length variation
* Inconsistent crease-line contrast

2. FINGERPRINT DEVICE

* Very shallow ridge structure
* Poor contact with laydown surface
* Plasticity across the image at laydown
* Poor registration of finger on contact surface

3. RETINAL PATTERN DEVICE

* Eyelash interference
* Inconsistent focus
* Poor eye alignment toward target
    -- lazy muscles
    -- tension
    -- drug induced

4. VOICE VERIFICATION DEVICE

* Speech impediments: stuttering, etc.
* Non-familiarity with the English language
* Laryngeal variations
    -- colds, post-nasal drip
    -- muscle laziness

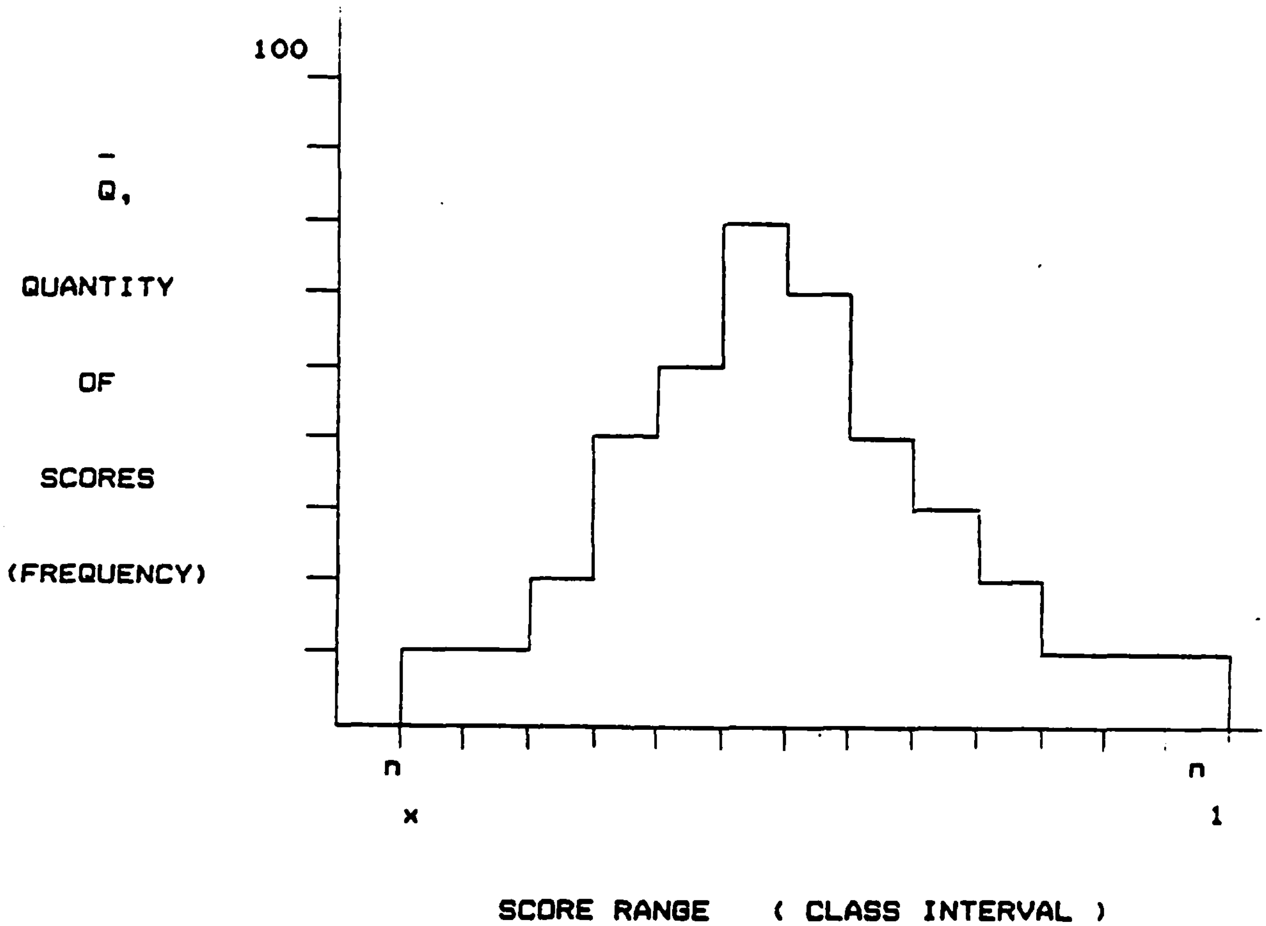


Figure 3-3: TYPICAL USER SCORE DISTRIBUTION CURVE

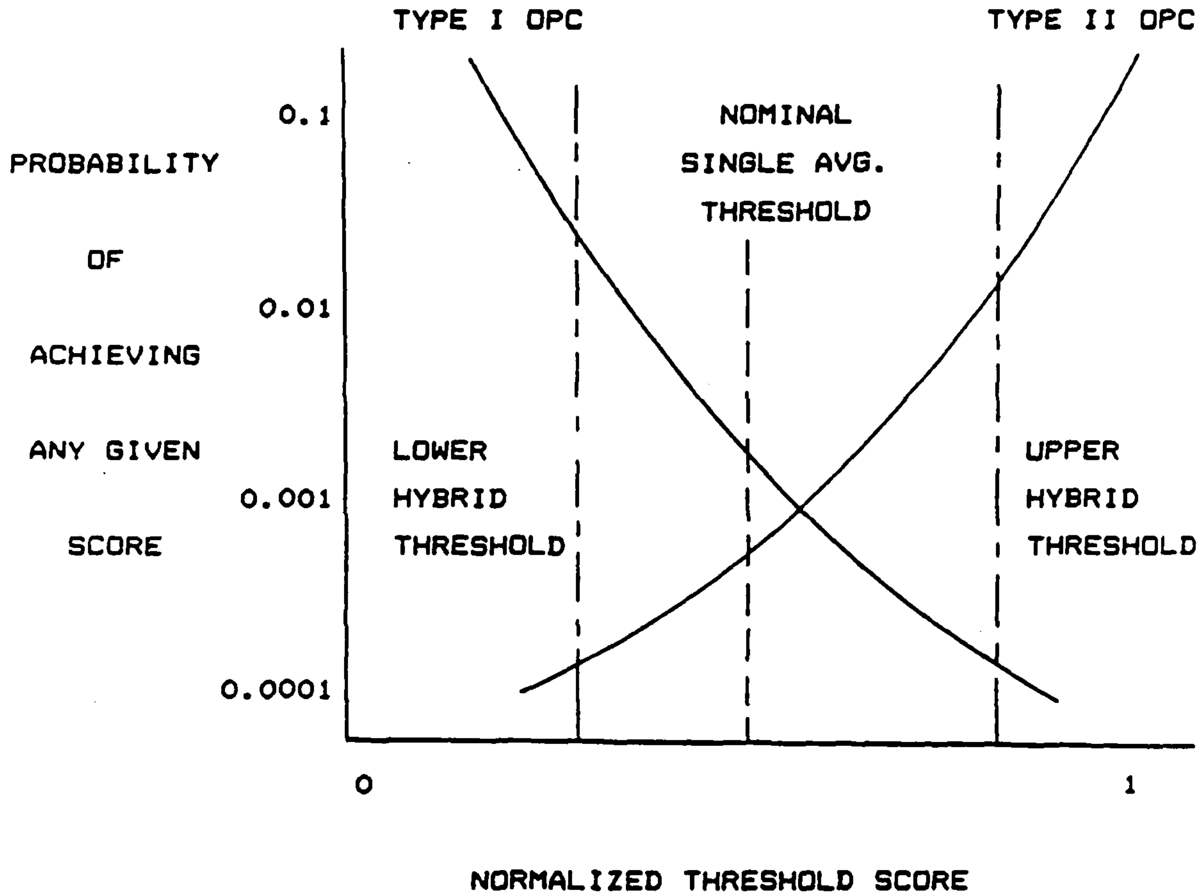


Figure 3-4: TYPICAL DEVICE ERROR PROBABILITY

verification attempts. The threshold setting determines this number, and the threshold setting is placed at a given Type II error position. The probabilities of obtaining a Type I or a Type II error from any device are plotted as typical numbers in Figure 3-4. It can be seen that if the value of the nominal threshold score is moved leftward (toward zero) the device is operating at a larger Type I error point on its operational performance curve, and at a lower Type II error point. Normally, a single PIV device has its threshold value adjusted to a fixed level so that its Type I/Type II error statistics are also fixed. In a Hybrid system, however, the threshold value can be advantageously set within a range of values, perhaps at different levels for each of the PIV types involved in the Hybrid. Figure 3-4 shows a lower hybrid threshold and an upper hybrid threshold, within which range of settings a dynamic value can be found, depending upon the verification criteria desired. Over this range, a particular value of Type I error can be traded off against the value of the Type II error at the same threshold score setting. The two curves have the relationship that any improvement in the value of one error type, obtained by changing the threshold, is gained at the expense of the other.

This relationship holds true for all known PIVs. The "x" nature of the crossover points for each PIV is similiar; the difference is primarily in the slope and the error probability value at the crossover.

The exact slope of the two curves at probability values below crossover is sketchy, given current levels of empirical data. A data point is available at the 0.1% level, for example, only once in one thousand verification attempts, on average. Where the quantity of data points is low, the curves are typically defined by extrapolation, which gives rise to curve-fitting procedures, and leads to throw-outs of data in the

category of "non-meaningful". The extent to which current Type I/Type II curve information has been subjected to throw-outs is unknown.

The data points contributing to the region below crossover can be considered as including those people from Figure 3-2 whose scores are consistently poor because of the reasons in Table 3-2. These users have been defined as "goats" on any single PIV type. A person is a Type I goat if he is unable to obtain a consistently good score when he attempts to match his own characteristics. His mean score is considerably removed from the mean score of the population. Similiarly, a Type II goat is a person whose scores when matched against others in the reference file are sufficiently poor as to be skewed into the Type I region of the X-curves. Generally, goats have the impact on the operational performance curves shown in Figure 3-5. The two curves are propped up to artificially high levels of error, compared to what they would be if goats were removed from the verification process. Since scores are constantly poor, no improvement in performance due to re-enrollment, learning curves, etc., can be expected, and the shape of the OPCs in that region are largely unchangeable. Although no hard and fast data on the segment of the population brandable as goats is available, if such were to be removed, improvement in the OPCs, upward of an order of magnitude, may be realizable, considering technology improvements, processing improvements, and the like.

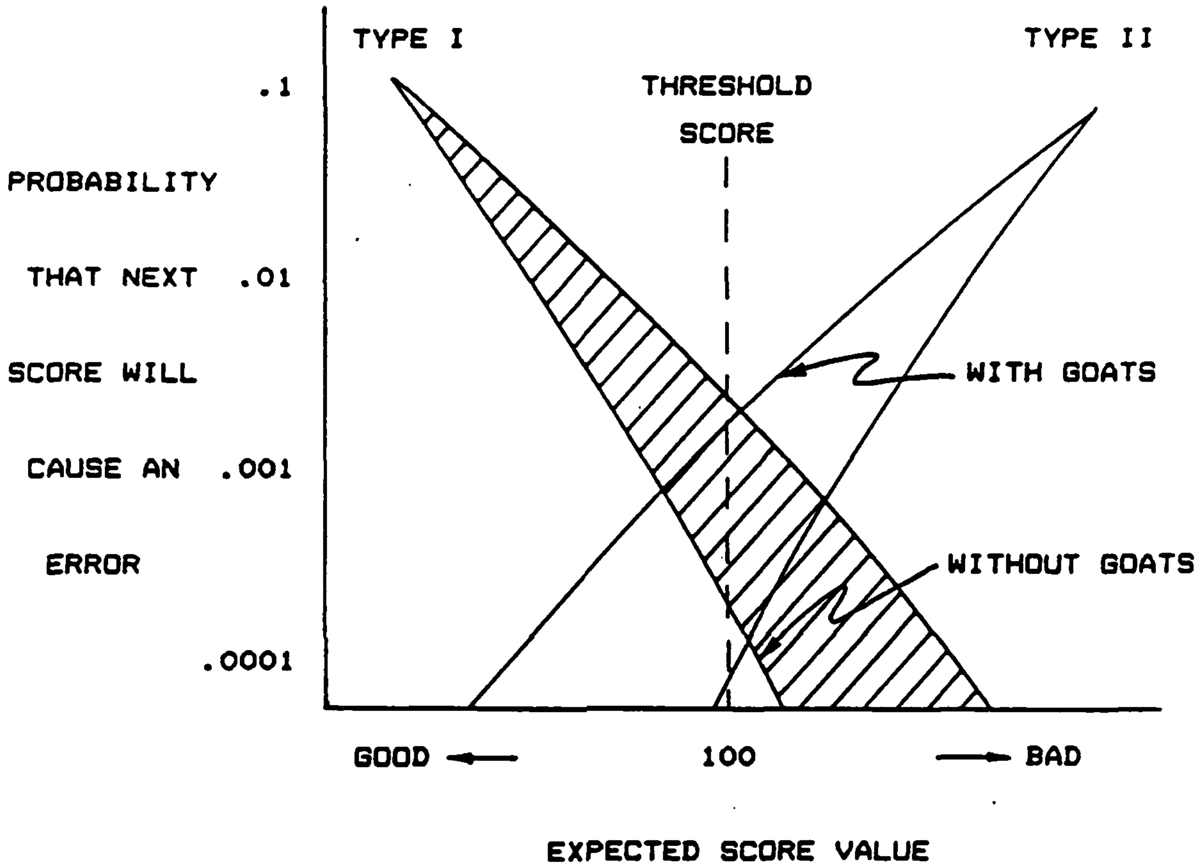


Figure 3-5: TYPE I/TYPE II ERRORS IF GOATS ARE FLAGGED

SECTION 4

HYBRID INTERFACE UNIT

A. FUNCTIONAL OVERVIEW

A Hybrid Interface Unit (HIU) is required in the portal in order to perform the data management and other functions necessary to support the hybrid concept. A listing of the general functions relevant to Hybrid action is given in Table 4-1. From a perusal of these functions the conclusion can be drawn that a miniature data processor is required. A more detailed review of the tasks, including a more specific definition of the algorithm required to give optimal performance, shows that the proper mechanization of the interface unit is a single board microprocessor of the type currently available for under $1000, including I/O chips and RAM memory devices. A diagram of the microprocessor configuration is given in Figure 4-1, indicating the appropriate connections via an internal data bus by which the necessary information is passed around inside the portal and to/from the Host Computer. The Central Processor Unit houses associated ROM chips capable of giving the HIU self-initiation and capable of holding the entire HIU run program including the Hybrid Algorithm. An overview of the sequence of events carried out by the executive run program is given in Figure 4-2.

B. HARDWARE CONSIDERATIONS

1. COMMON BUS

The diagram of Figure 4-1 indicates the relatively large quantity of peripheral devices with which the HIU must

TABLE 4-1

HIU GENERAL FUNCTIONS

1. Receive card reader data and acknowledge same
2. Perform card authorization
3. Find the file name from the authorization list
4. Set direction of portal entry/exit
5. Perform timing of PIV operations/portal operation
6. Interface with the entrant via display
7. Interface with Portal subsystem controller unit
8. Compare file name and PIN
9. Interface with ICP via a Hi-Speed data link
10. Send the Standard file request to the ICP
11. Receive and unpack the standard file via interrupt
12. Perform device sequencing operations
13. Interface with each PIV
14. Configure hybrid and execute decision algorithm
15. Transmit the accept decision to the door opener
16. Transmit the reject decision to the Host for further processing
17. Acquire raw data, each PIV
18. Format the transaction record
19. Transmit the transaction record
20. Report faults in constituent operations
21. Report on device degradations
22. Provide overrides when commanded
23. Prioritize the various interrupts
24. Send the proper alarm code on any of the above
25. Receive new Order-of-the-day (OOD) via interrupt
26. Unpack and overlay OOD in RAM
27. Receive new Authorization Table via interrupt
28. Unpack and overlay the authorization Table in RAM
29. Provide default settings within the portal

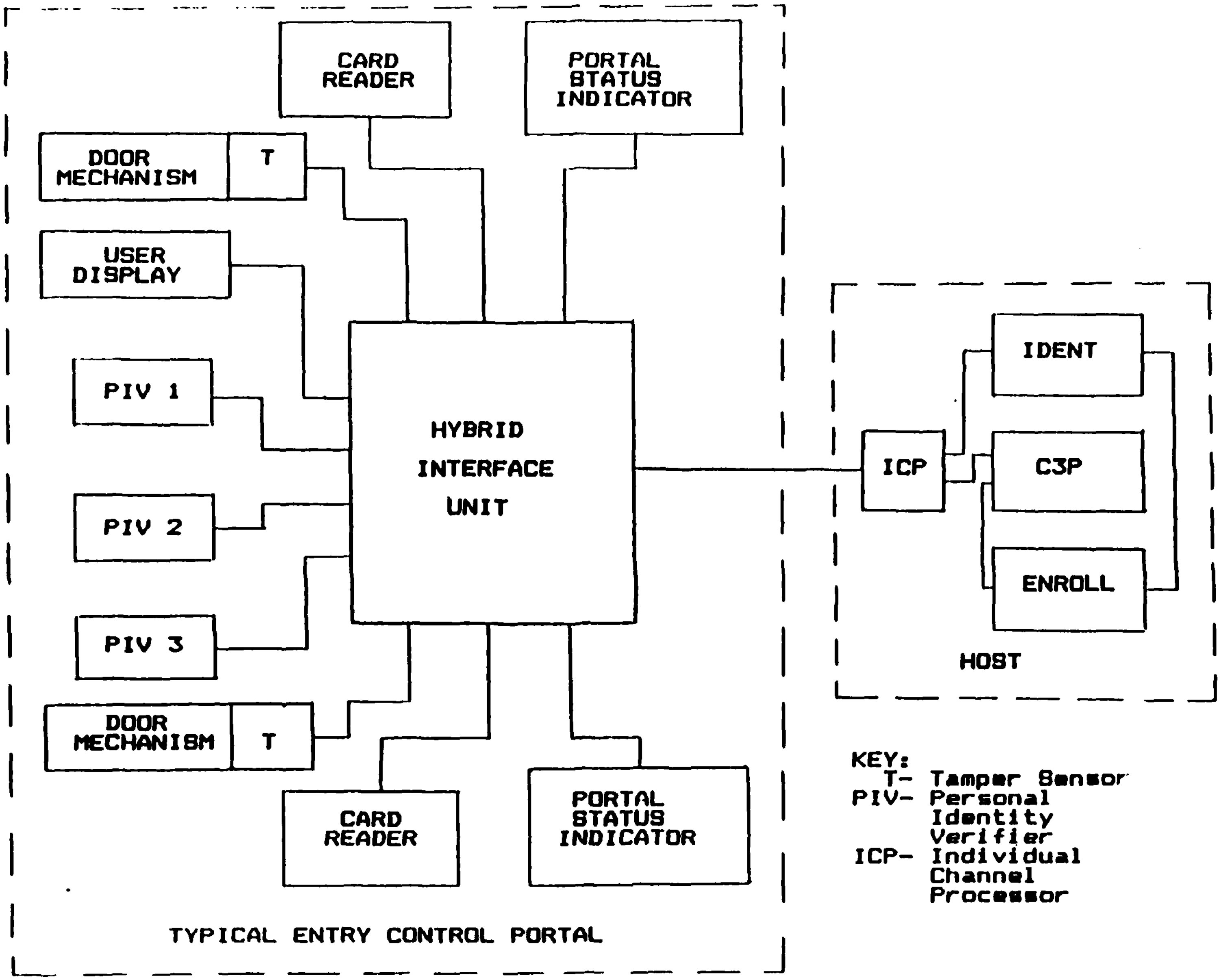


Figure 4-1: HYBRID ENTRY CONTROL SYSTEM; INTERFACING STRUCTURE

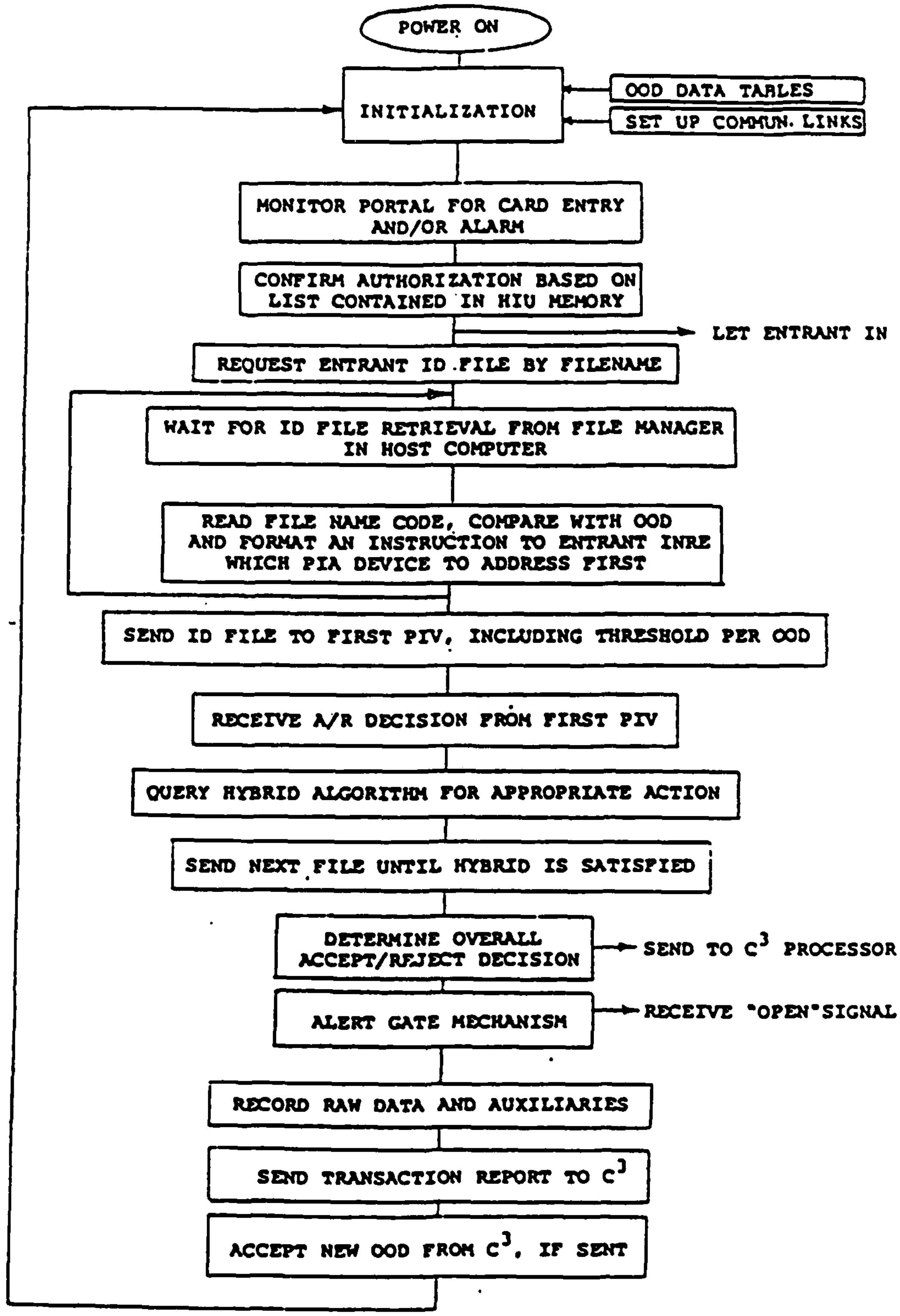


Figure 4-2: EXECUTIVE SEQUENCE; HIU SOFTWARE

communicate in the typical portal. The I/O function is designed to be achieved using serial input/output chips or parallel input/output chips, each connected to the CPU by a common bus. An 8-bit bus is considered satisfactory in that single byte data is typically passed through the I/O channels. Matching baud rates to each PIV device is possible using executive programming of the SIO/PIO devices at the HIU end. Sufficiently high transfer rates are achievable to accommodate full data transfer to/from the peripheral internal to the portal in under a second, and in most cases within a fraction of a second.

2. CPU TYPE

The characteristics required of the CPU chip are consistent with any of the 8/16 bit devices available today. Typically, the CPU should be capable of performing 200,000 instructions per second, not a severe requirement in today's state-of-the-art. The intent is to move data quickly to the appropriate PIV, Host, or to/from memory, as required.

The CPU must be capable of nested interrupts, so that any interrupt routine currently in operation can itself be interrupted by a higher priority function, such as an alarm. The original interrupt routine must wait and resume when the higher priority interrupt has run its course and relinquished control. Most CPU's permit such interrupt level designation.

3. MEMORY SIZE

Dynamic RAM is available in low cost chips of 64K bit size. All tables, reference and raw data formats and cache memory should fit within 64K bytes. Other storage includes ROM, expected to be useful in housing the executive and I/O driven programs, all within an 8K byte size. Disk storage is not

considered to be a requirement, nor is DMA, within the HIU.

4. DISPLAY

The display must be given easy-to-understand messages by the HIU for the user, of such timeliness and specificity as to maximize throughput. The centralized single display offers the most information per unit time and reduces the confusion to zero on the part of the entrant about where he should be looking for further instruction. Visual symbolism offers the best understanding sooner to a wider range of the population. It is important to throughput that the complete gamut of instructions are conveyable to the entrant as each personal need is met in the portal. Verbalizing instructions will help to augment the symbolism and to steer the user back to the correct decision-path if he strays, without losing control. A number of display types incorporating text and graphics are available for use in the design to perform this function, and are easily adapted to a serial or a parallel output channel from the HIU. The problem of tracking the entrants progress through the portal and giving the correct series of messages to the display belongs to the HIU algorithm, which is oriented towards reaching the accept/reject decision in the fastest manner inside the portal. The tracking operation must confirm the users procedural position so that precisely the correct message is issued to the display.

5. PIV INTERFACES

The number of interconnects to/from a single board microprocessor is limited more by the hardware space available on the board to pull off connectors than by the electronics or the software. Even a rudimentary SBMP has a level of 16 I/O ports electronically addressable with ease, which level appears to be adequate for the HIU. The I/O ports are designed to be modular

in boards, which are insertable into slots in the motherboard comprising the common bus. The extra ports are brought on line either by completing switch positions or by inserting replacement ROM's into the SBMP, or both.

The baud rate of each serial interface in the HIU is required to be programmable from 9600 baud upwards to 76.8 KBAUD, in order to send and receive reference data and raw data across the interface with as little overhead time as possible. Typically, baud rate is set by the ROM during the initialization process.

Error checking is recommended, in accordance with any of the standard procedures, for the purpose of permitting an instant retransmission of a selected portion or all of the data.

6. CARD READERS

The user can confirm his authorization to enter the portal by using his unique number, assigned at the time of enrollment, applied via a card reader if the number is invisibly placed on a badge pass, or as a remembered number. A card reader does not appear to have signifigant advantages over the keypad from the security position, since both are dwarfed in their discrimination capability by the Hybrid System, and each has its disadvantages. In the long run, it may be that the deciding factor for selection in the Hybrid System is the reduction in nuisance reponses that one or the other provides in any given operational environment. These include fewer instances of:

.. any user making a demand on the guard because of a forgotten badge or number

.. down-time at the portal for maintenance operation on the devices (including sabotage)

.. casual entry attempts, in the face of such a high probability of undergoing detention.

The case can be made for universality in the authorization call-up equipment, in order to use more easily remembered passwords as opposed to number combinations. Equipment is becoming available at low cost to enter all alphanumerics, and the day is approaching when the spoken word will be decoded giving rise to a multiple phrase password.

It would seem desirable to keep lifetime costs as elemental tradeoffs in the selection decision, and at this point in time, also to avoid freezing any single device type or manufacturer into the design. Keeping all options open also allows for those portal configurations where authorization and identification can both occur inside the portal.

7. TIMING OF PROGRESS IN THE PORTAL

In a multiple PIV Hybrid, the Hybrid Interface Unit becomes the most important part, as it directs user activities in the portal, controls throughput, computes margins by which to accept or reject, and makes the decision to admit the user or to formulate an alarm message containing rejection data for transmission to the Central Security Office for further processing. This set of sequences was shown in simple form in Figure 2-1. The algorithm has been defined to be able to work with any PIV type which meets the basic requirements in Section 3.

The overall in-portal time is subject to user control, but it is the intent of the HIU algorithm to monitor progress and to speed him through the sequences. It can be expected that as the gamut of sequences is learned by the user, his in-portal time

will settle out to a nominal value. It can also be expected that the in-portal time performance will have a population spread profile similar to the error performance profile; some users will be super-achievers and others will have severe difficulty in making progress through at least one of the sequences.

For analytical purposes the major tasks inside the portal are broken into time segments as shown in Figure 4-3. Nominal values, in seconds of elapsed time, are given, and within any segment a dashed/solid line indicates estimates of a breakpoint between fastest and typical traverses through the segment for a three-PIV set. It is the intent of the HIU algorithm, in concert with accompanying design features in the Host, to create, as much as possible, an overlapping of sequence segments so that processing delays, as opposed to user movement time, are minimized. For example, the user is directed immediately to a second PIV in the sequence after scanning has been completed on the first PIV, with no waiting to see the results of the first activity. The algorithm senses the progress and directs an immediate advance to the next level. In this way, the processing time of one PIV overlaps the scanning time of another.

It is pertinent that portal throughput automatically becomes lessened as more PIV's are added to the sequence. This puts pressure on the non-PIV time segments in the design, pushing towards lessened periods for their execution. These non-PIV segments include such portal elements as door opening, closing and latching times, positioning time for weight measurement, PIN key-in time, quantity of retrials permitted on any in-portal segment and the like. As a rule-of-thumb, every second that can be lopped off a 20-second throughput time would be equivalent to eliminating a complete portal in a 20-portal configuration, other factors being equal. This translates to an approximate cost of $100,000 per second.

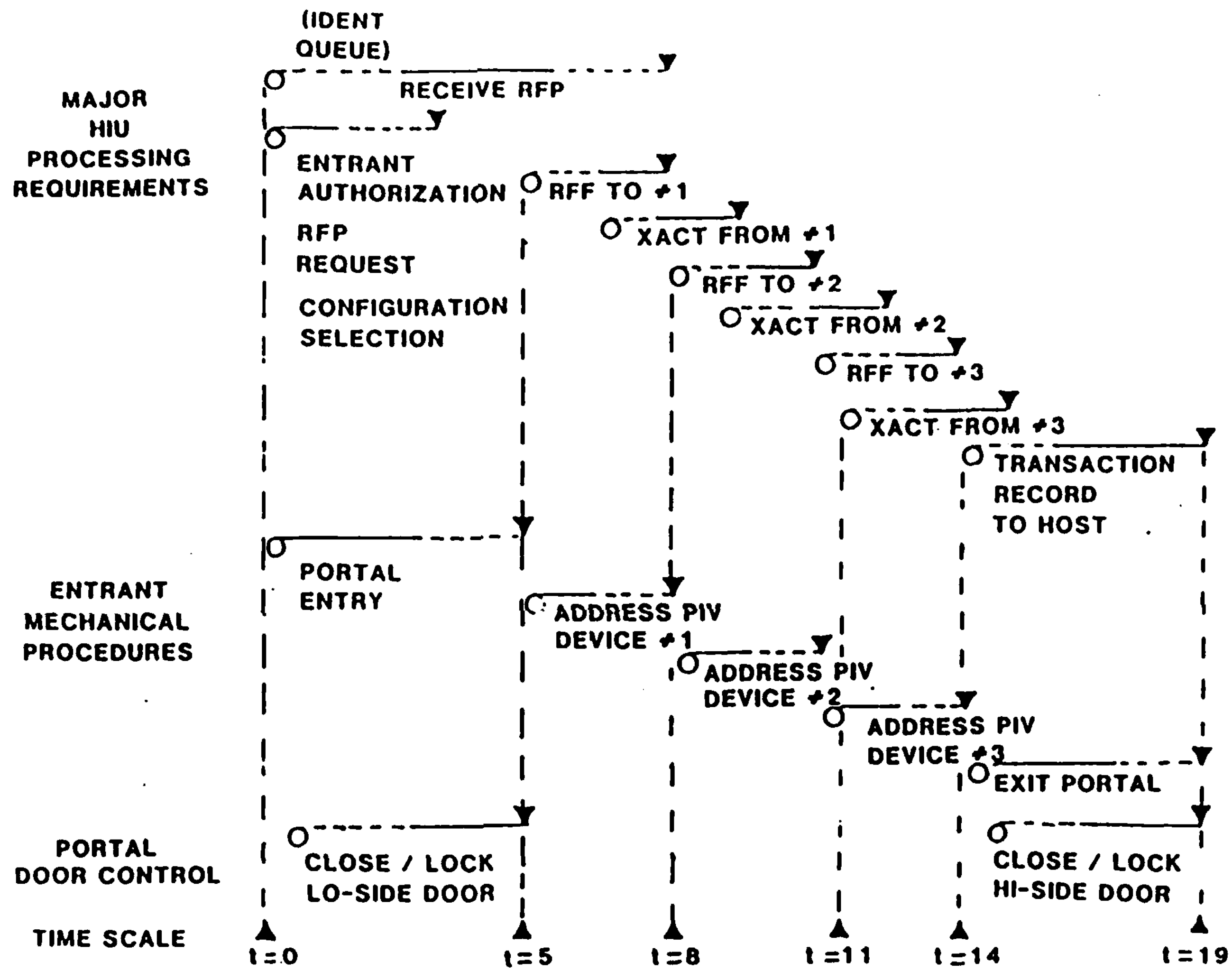


Figure 4-3: PORTAL THROUGHPUT TIMING ANALYSIS

Obviously, any delay in the receipt of the Reference File Package from the Host owing to a queue at the IDENT Processor or to an excessive transmission time is to be avoided. The design of the configuration in the Host and in the Data Link requires sufficient speed to avoid these delays. This problem becomes more acute as overall Reference File Package size increases, as with future PIV's being added to the system.

It should be noted that unnecessary delays in sending the raw data on the return path to the Host are equally important to throughput. With proper use of store-and-forward techniques in the data channel, these delays can be minimized towards zero. The contribution of the C3 Processor queue in receiving the raw data may be sufficient under unusual loads to warrant the throwout of stacked-up raw data until the queue diminishes and the system becomes self-correcting. This is undesirable, but possibly necessary.

8. DATA LINK

Figure 4-4 shows the relationship between Reference File Package size in kilobytes and its transmission time in seconds using different baud rates between the HIU and Host. For anticipated file sizes of 20 kilobytes, the transmission time of about 4 seconds is realistic, if 76 KBAUD is programmed. A four-second period appropriately overlaps the portal entering time and the initial instruction reading time allocated to the user, so that this level of transmission time is transparent to the user. However, if programmed baud rate between the HIU and Host is dropped to 9.6 KBAUD, the overlap disappears and the delay becomes untenable. Although a reduced file size would improve the situation, any PIV configuration containing Voice Verification is not likely to permit reduced file sizes. The trend in future PIV configurations is toward larger files, not

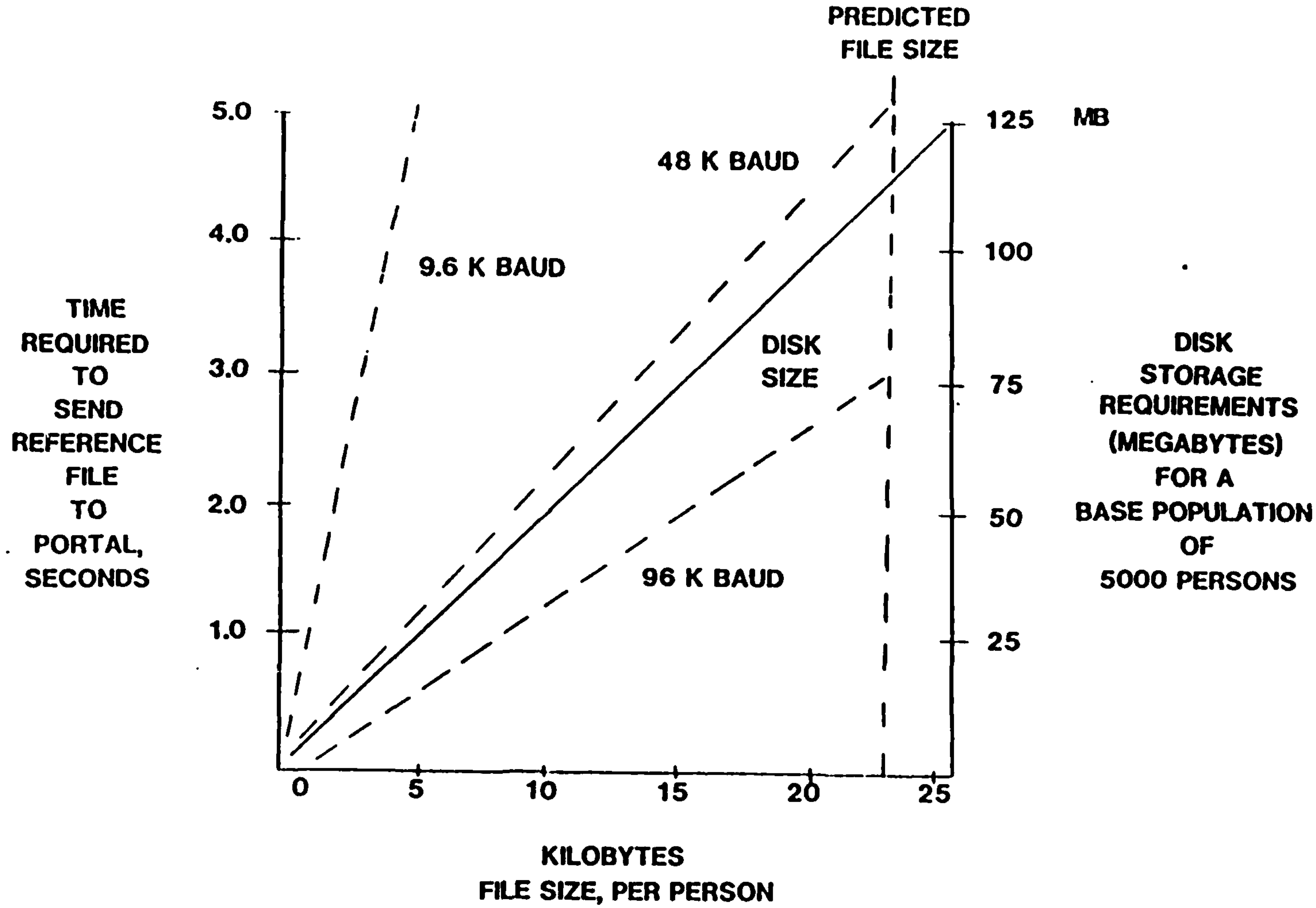


Figure 4-4: IMPACT OF LARGER COMBINED REFERENCE FILES

smaller, as larger numbers of PIV's are placed in the portal, and as more of them measure behavioral characteristics, each certain to require larger chunks of reference data.

9. INDIVIDUAL CHANNEL PROCESSORS

At the Host end of the Data Link, the Hybrid design requires an Individual Channel Processor capable of insulating data to/from the portal and the distributed elements of the Host. A diagram of a typical ICP is shown in Figure 4-5. A form of single board microprocessor, it acts to buffer the reference file package retrieved by the DMA circuits in the IDENT Processor, prior to shipping the file to the HIU in the portal. Similarly, it buffers raw data enroute the Host to the HIU. Overall, its function is to avoid the double impact of queueing and time consuming data transmission, and to serve as a multiplexer to the ditributed elements of the Host. As shown in Figure 4-6, the twin busses permit the file retrieval process to operate independently of the raw data collection process. The execution protocol in the ICP helps prevent bus interferences from arising, and permits alarm processing to override the bidirectional flow of files and raw data, as required.

C. HYBRID ALGORITHM

The HIU is responsible for gathering data at the portal during an entry attempt, assimilating that data, generating an accept/reject system level entry decision for use in the portal and reporting the results of the reject/transaction to the Host. This is accomplished with the Hybrid Algorithm. Figure 4-7 shows in block form the relationship of HIU algorithm processing to the essential processing within the Host defined as the Performance Control Algorithm. In effect, the HIU algorithm is the loop portion of the Performance Control Algorithm carried out

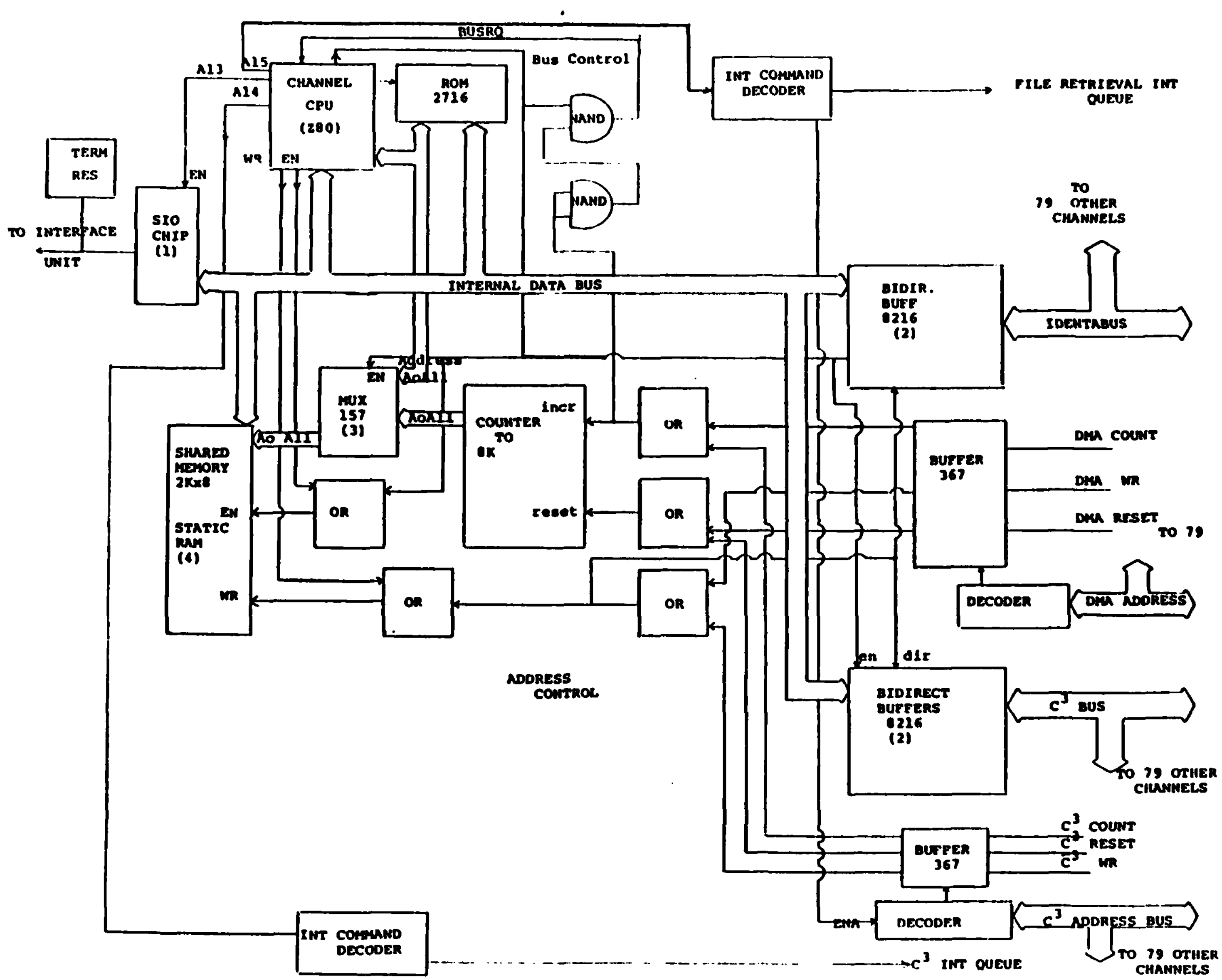


Figure 4-5: TYPICAL INDIVIDUAL CHANNEL PROCESSOR CONFIGURATION

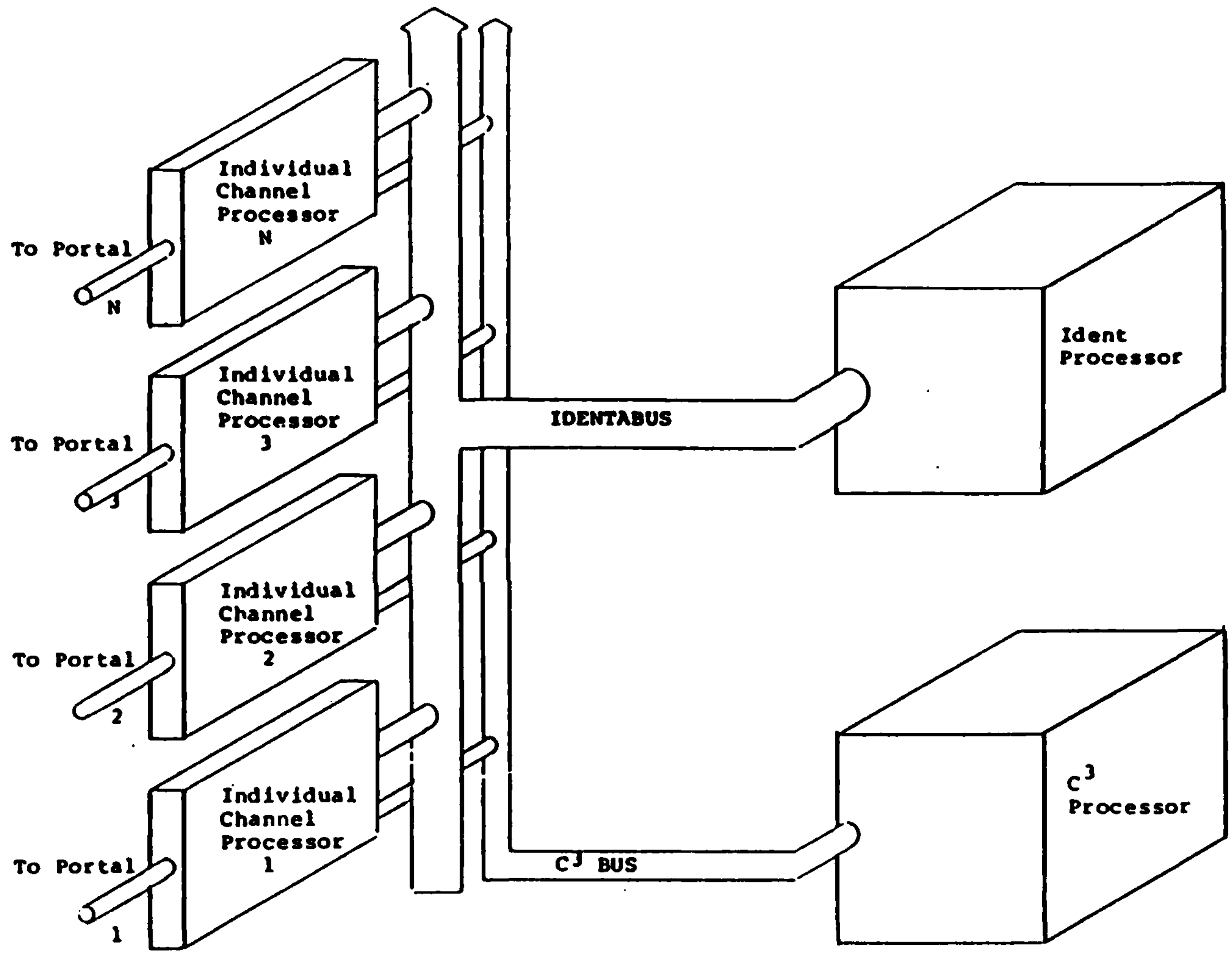


Figure 4-6: ORGANIZATION OF INDIVIDUAL CHANNEL PROCESSOR IN HOST COMPUTER

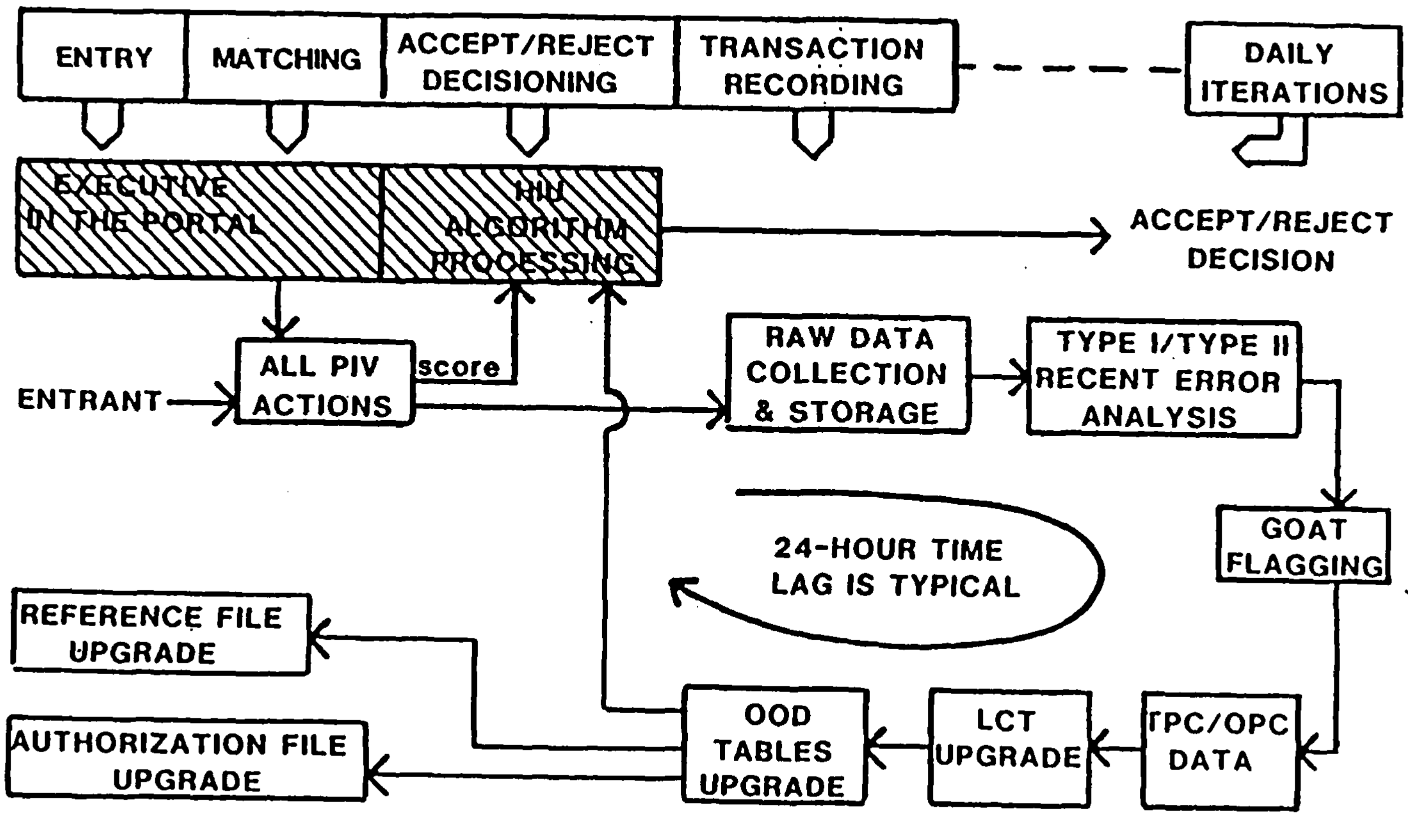


Figure 4-7: THE HIU ALGORITHM WITHIN THE PERFORMANCE CONTROL ALGORITHM

in the HIU, and the additional housekeeping routines connected with the portal entry/exit task.

The hybrid algorithm is initially defined by four major tasks: standby operations, user authorization, user identity verification and transaction recording. The block flow of these tasks is given in Figure 4-8.

1. STANDBY OPERATIONS

While waiting for an entry attempt, the hybrid algorithm forces the HIU to continually monitor its environment. All PIV devices, as well as the HIU itself, are required to undergo self test. This also provides the status of the communication links with these devices. All tamper sensors are tested, as are the door mechanisms and card readers. If any deviations are encountered, the Host is alerted as to the nature of the problem, and the portal may be placed into an offline condition. Figure 4-9 represents this task in flowchart form.

2. USER AUTHORIZATION

Access to the portal, and thereby to the PIV devices, is granted only if a user is authorized to enter the secure area. An authorization decision is rendered as to the claimed identity of the user, found from the invisible number of his identification card, presented to him at enrollment.

The decision process, represented in flowchart form in Figure 4-10, requires an authorization table to be resident in working RAM memory in the HIU. This table, supplied by the HOST via the ICP contains the identity of all users authorized to gain access through this portal, and their time zone(s) for the

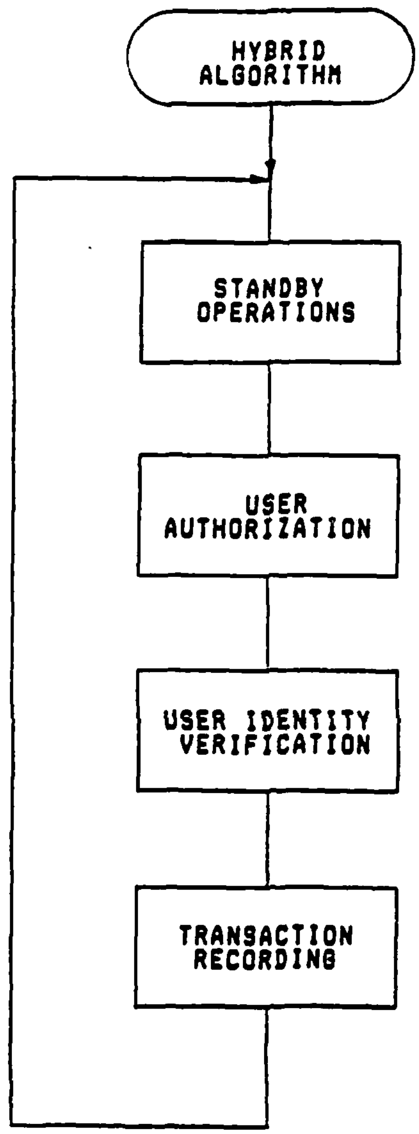


Figure 4-8: HYBRID ALGORITHM; MAJOR TASK FLOW

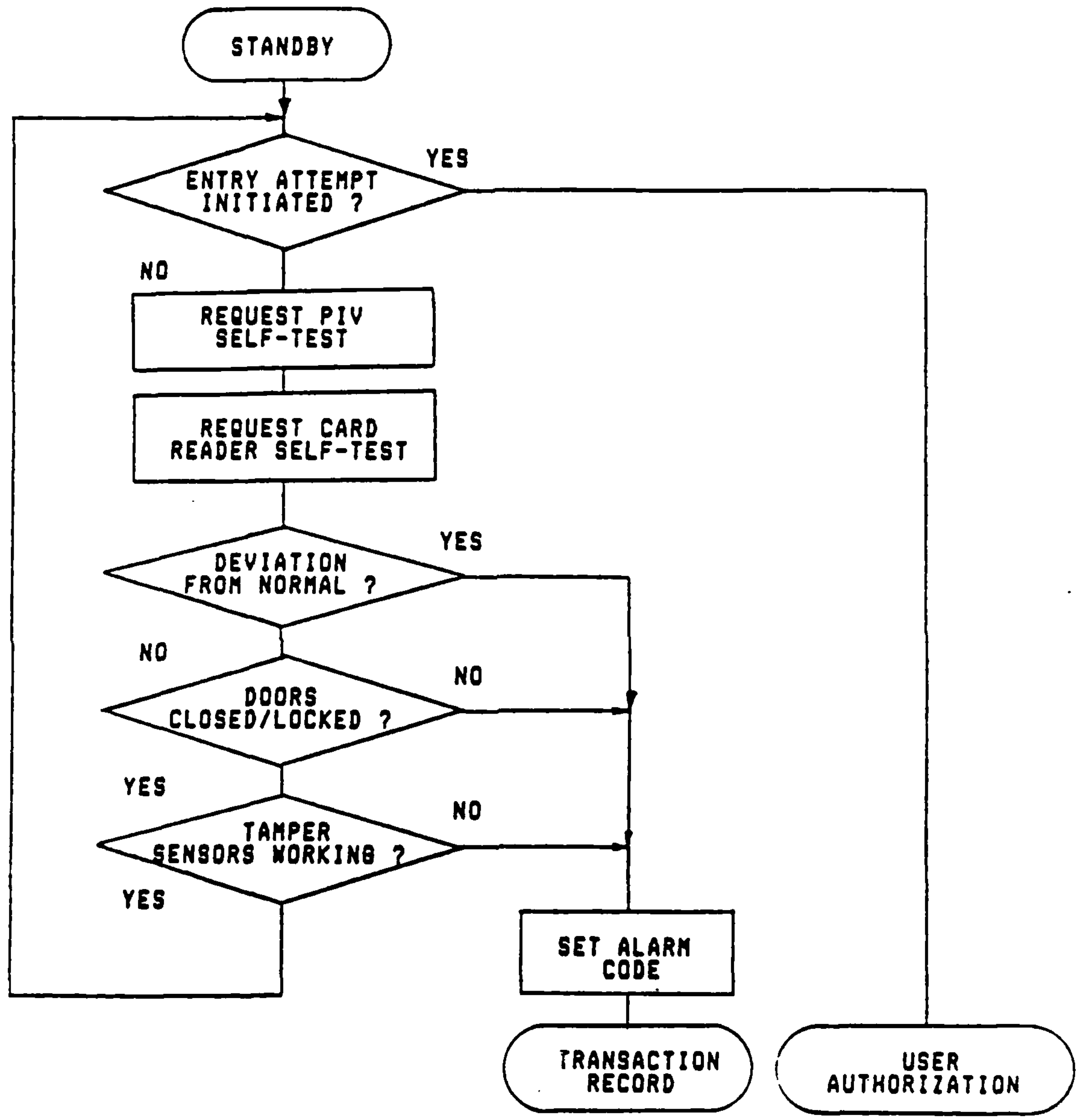


Figure 4-9: HYBRID ALGORITHM; STANDBY OPERATIONS

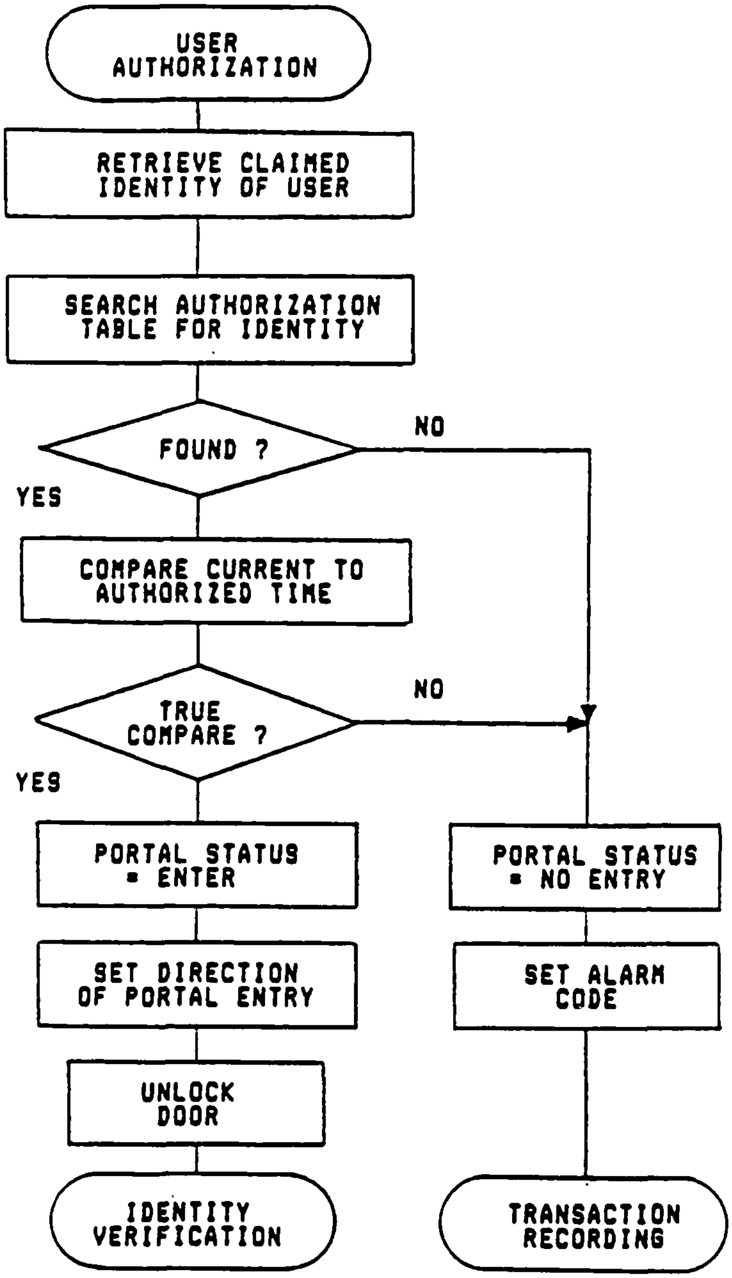


Figure 4-10: HYBRID ALGORITHM; AUTHORIZATION DECISION PROCESS

current day. This table is updated at least once a day from the Host.

A user is said to be authorized to gain access if an entry exists in the authorization table that matches his claimed identity, and the current time is an authorized time for him to enter. If the user is authorized to enter the secure area, the appropriate side of the portal is unlocked, and access to the PIV devices is granted. If the user is not authorized, portal (and PIV) access is denied, an alarm condition exists (albeit low priority) and the Host is alerted to the problem. Decision-making is simultaneous with card insertion, and introduces no measurable entry delay to authorized persons.

The authorization task is also responsible for setting the portal entry direction, ingress vs. egress, in order to sequence the appropriate doors and to enable the identity verification task at entry. With programming changes, this routine could also enable the PIV for use at exit, if desired.

3. IDENTITY VERIFICATION

Entry from the portal to the secure area is granted only if a positive identity verification is made. This portion of the hybrid algorithm is responsible for PIV device sequencing, reference feature file retrieval, raw data acquisition and hybrid configuring. The block flow of the identity verification procedure is represented in Figure 4-11.

In this design description, identity verification is only required at entry, not exit, through the portal.

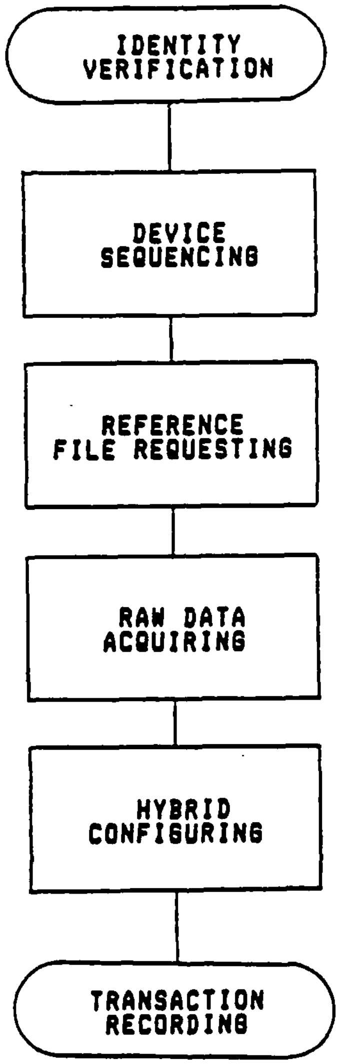


Figure 4-11: HYBRID ALGORITHM; IDENTITY VERIFICATION BLOCK FLOW

A. DEVICE SEQUENCING

This portion of the identity verification task of the hybrid algorithm sets the sequence in which the user is to address the PIV devices and the order in which the host is to return the device reference feature files for user ingress through the portal.

If the user is requesting egress through the portal, via Reader No. 2, the hybrid algorithm branches (not shown in Figure 4-11) directly to the transaction recording task.

Refering to Figure 4-12, a device sequence code (DSC), given in the OOD, forces the manner in which the device sequence is obtained. The DSC directs a predetermined sequence to be used if all users are commanded to address the PIV devices in the same order for data collection purposes. If the OOD does not require a commanded sequence, the sequence for each user is based on his proficiency rating. When throughput is desired to be at a minimum and the Type II error rate is not critical, the user may not be required to address all of the PIV devices in order to verify his identity, and the latter sequencing procedure may be called by the HIU.

The algorithm requires the user to be inside the portal before the sequence is displayed. This condition is initiated by opening the portal door. This operation is also timed, and, if the door is not opened within a limited time period, an alarm condition exists, and the host is notified.

B. FILE REQUESTING

The identity verification task requires the HIU to retrieve the reference feature files (RFF) from the host. The request is

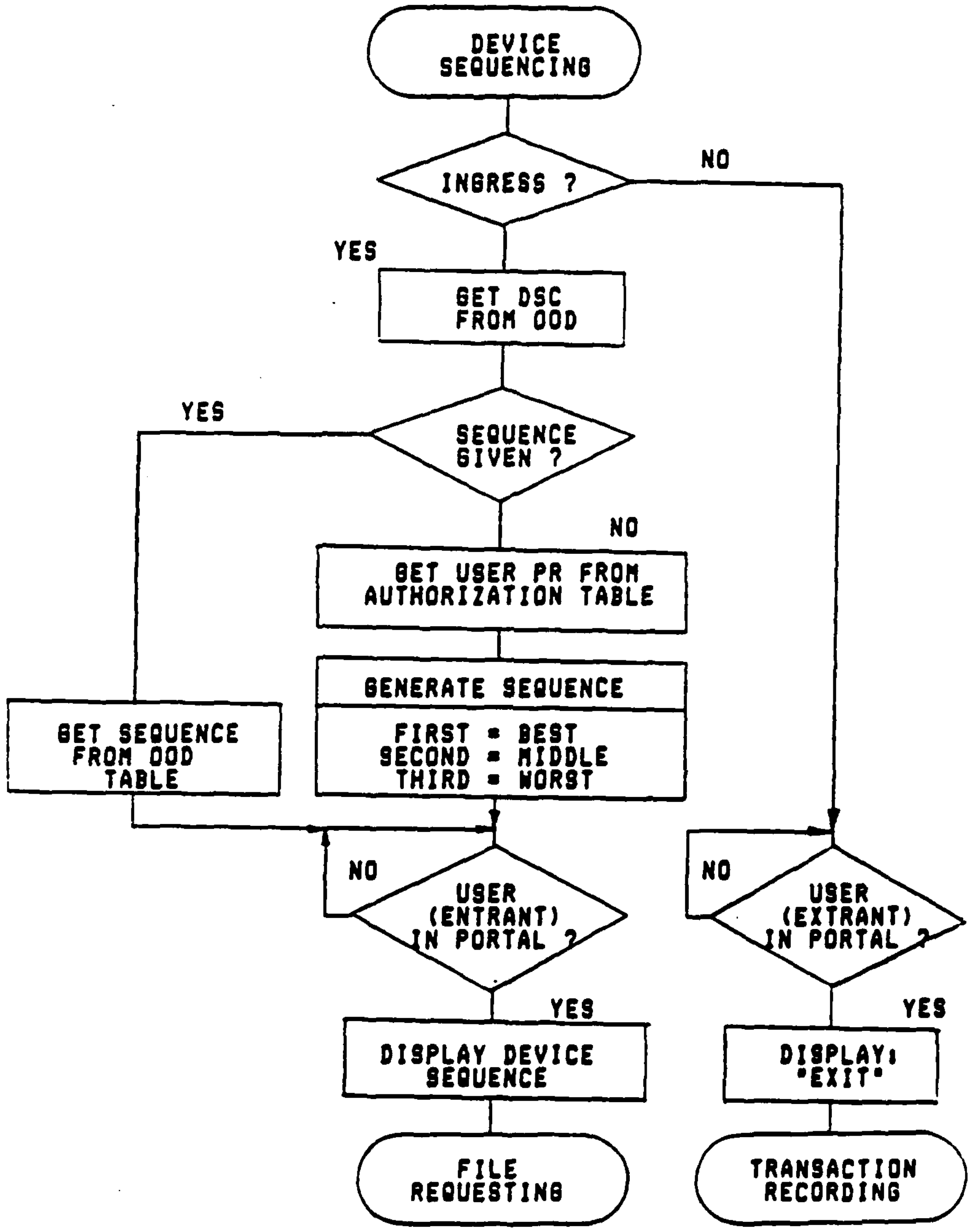


Figure 4-12: HYBRID ALGORITHM; DEVICE SEQUENCING DURING IDENTITY VERIFICATION

formatted in such a manner that the ICP return the RFFs in the order that the user is to address the devices. There is one stipulation, however; if a user is defined as a Type II goat on any PIV, that RFF is not transmitted to the HIU.

Figure 4-13 is a representation of the file requesting procedure. Table 4-2 shows the contents of the request table necessary to define the file required, the RFFs to be returned and their order.

The identity of the user is required in the table. It is the reference file package (RFP), by title, that the IDENT Processor retrieves from disk and transmits to the ICP. The ICP in turn transmits the RFFs contained in the RFP, to the HIU in the order given in the device sequence entry in the request table. If, however, the goat code entry is a number other than null, that RFF is skipped, i.e., not transmitted to the HIU.

The actual request (transmission of the table) does not occur until the portal is occupied, i.e., the user is in the process of entering the portal.

C. RAW DATA ACQUIRING

From the PIV device's standpoint, the HIU is their host. Each device need only receive an initiation signal from the user, perform one valid raw data acquisition, and the user advances to the next device. The current device will then receive the reference feature file from the HIU, generate its device level score and return its transaction record. The PIV device has completed its job.

Refering to Figure 4-14, the raw data acquiring task in the HIU is responsible for passing the RFF through to each device as

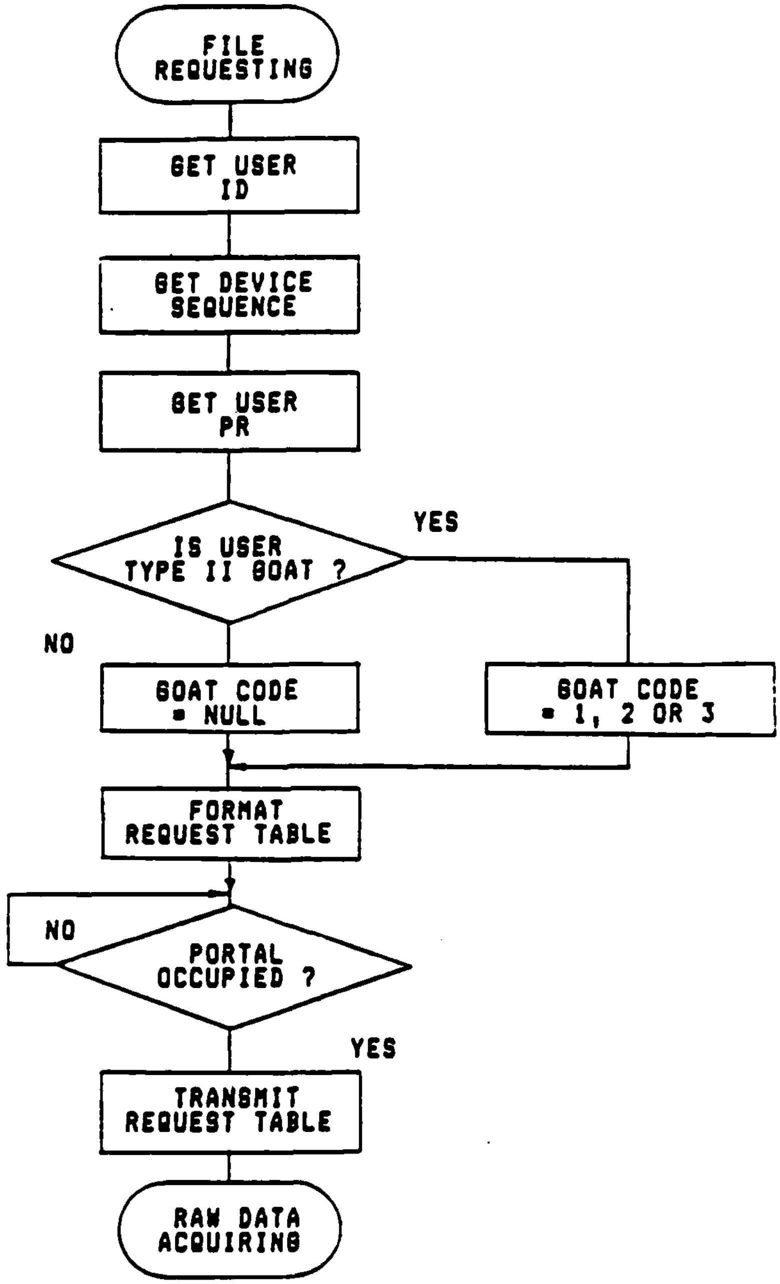


Figure 4-13: HYBRID ALGORITHM; FILE REQUESTING DURING IDENTITY VERIFICATION

TABLE 4-2	
DATA TRANSMITTED TO HOST FOR REFERENCE FEATURE FILE REQUESTING	
CONTENTS	REMARKS
1) USER ID	* This is the invisible number read from the user's ID card.
2) DEVICE SEQUENCE	* The order in which the RFFs are to be returned is defined in this entry.
3) GOAT CODE	* Any RFF not to be transmitted will be labeled here -- (null => send all, 1=> don't send first device RFF, etc.)

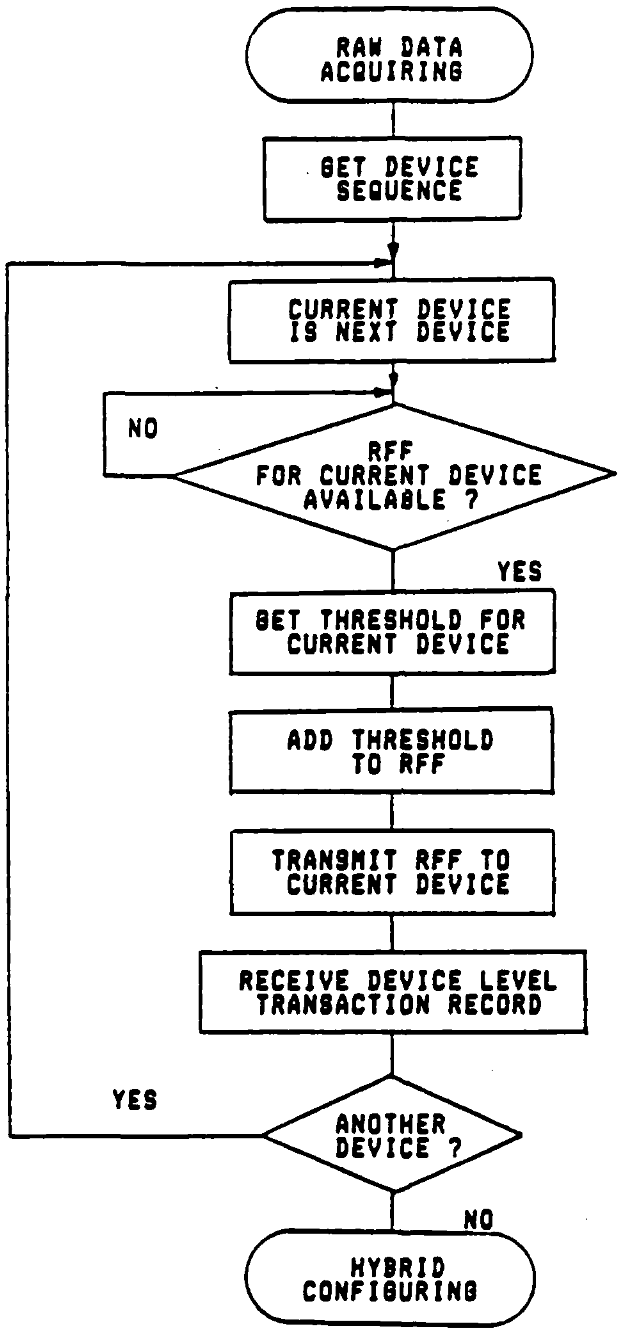


Figure 4-14: HYBRID ALGORITHM; RAW DATA ACQUIRING DURING IDENTITY VERIFICATION

they become available, and supplying the device with the commanded threshold score, if it is desired to do so and if it is different from the one currently being used by that device. The HIU then receives the device level transaction record in return.

Unless a raw feature set is required (if the device sequence code points to a given order), only those devices needed to fulfill the logical configuration need be addressed by the user. This information will be in the form of feedback from the hybrid configuring portion of this task.

D. HYBRID CONFIGURING

It is here that the system level accept/reject identity verification decision is generated. As the device level threshold comparisons to scores are made and the score margins are made available, they are combined in accordance with the commanded logical configuration (LC) until the decision is resolved. Figure 4-15 represents the decision process.

Based on the user's goat status, found in his proficiency rating (PR) - an entry in the authorization table, either the priority LC or a contingency LC is used to generate the A/R decision. The priority LC is preferred since it has been defined in the performance control algorithm as best fitting the given OOD. However, the contingency LCs will force equivalent error probability numbers. The required function of the contingency LCs is to get those users who have been defined as goats through the ECP.

As the PIV devices return their transaction records, the hybrid configuring procedure checks to see if the chosen LC can be resolved with the current quantity of data. As soon as it can be resolved, the procedure will end. Only if the devices must be

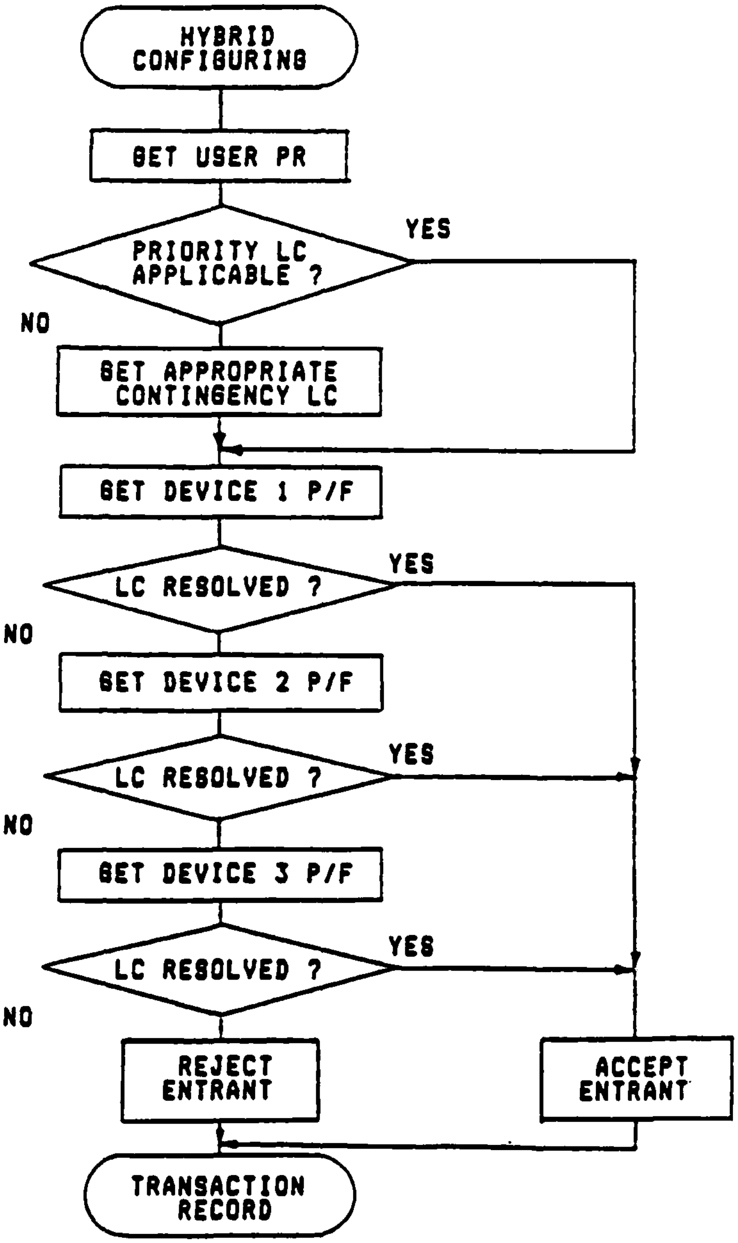


Figure 4-15: HYBRID ALGORITHM; HYBRID CONFIGURING DURING IDENTITY VERIFICATION

addressed (raw data required, three device LC, etc.) will they be. As has been shown, Table 2-1 indicates the symbolic combination resulting in overall system alpha and beta if certain candidate LCs are contenders to be the contingency set. Table 4-3 gives typical candidate thresholds to be inserted into the HIU algorithm if one of the selected usable overall system error pairs is mandated by the Base Commander's security requirement for the day.

When the A/R decision has been generated, the identity verification task within the hybrid algorithm is complete. Rejection of the entrant consists of notifying the Host, who takes further action to erase a lockup.

4. TRANSACTION RECORDING

Each of the preceding tasks (and sub-tasks) within the hybrid algorithm buffers all data necessary and sufficient to record the transaction. This task is required to transmit that data to the host and secure the portal before another transaction can take place.

Figure 4-16 represents the procedural flow, Table 4-4 defines the contents of the possible transaction records.

TABLE 4-3

TYPICAL LOGICAL CONFIGURATION TABLE

Selected Hybrid System Error Pairs for --
Device Combination #14: S1 AND (S2 OR S3)

Control BETA	Best Obtainable ALPHA	Corresponding Thresholds TS1	TS2	TS3
:				
:				
.0000004	- -	-	-	-
.0000006	- -	-	-	-
.0000008	.0065423	11	11	11
.0000010	.0048423	11	11	10
.0000020	.0025422	11	11	7
.0000040	.0013423	11	11	4
.0000060	.0008423	11	11	2
.0000080	.0006423	11	11	1
.0000100	.0006312	10	11	1
.0000200	.0006075	7	8	1
.0000400	.0006017	4	4	1
.0000600	.0006009	2	3	1
.0000800	.0006005	1	2	1
.0001000	.0006004	1	1	1
.0002000	- -	-	-	-
.0004000	- -	-	-	-
:				
:				

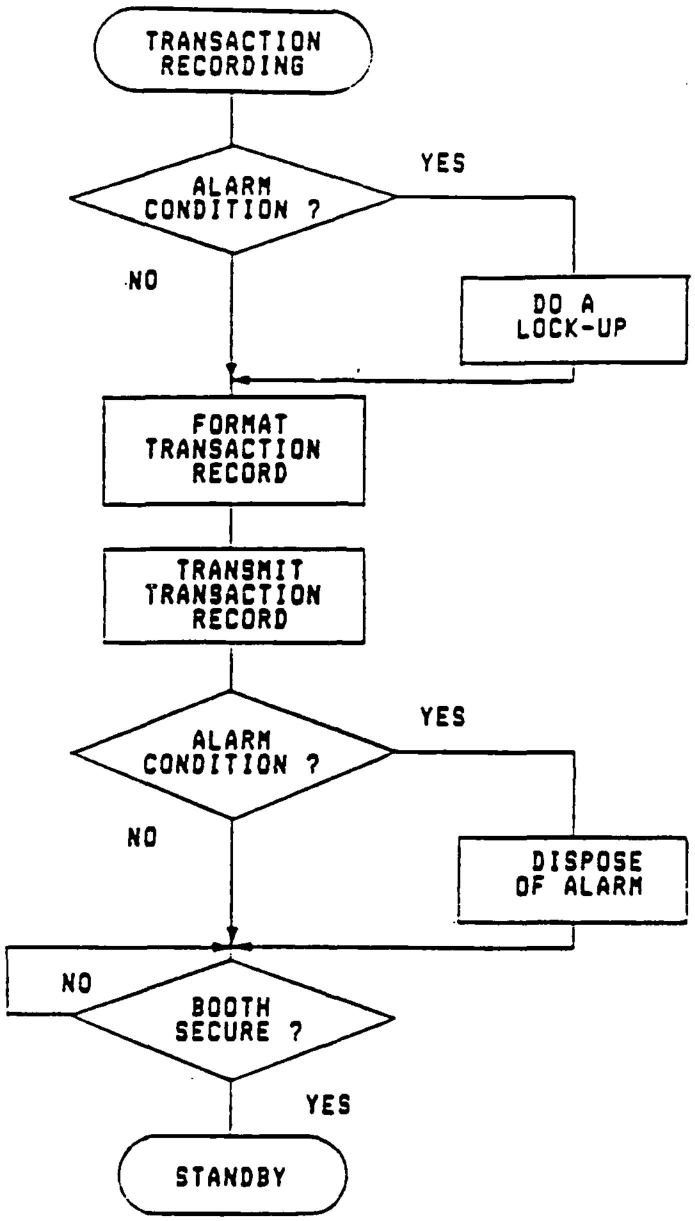


Figure 4-16: HYBRID ALGORITHM; RECORD OF TRANSACTION TO HOST

TABLE 4-4

TRANSACTION RECORD CONTENTS

BY PORTAL USEAGE RESULT

1) ENTRY GRANTED

* TRANSACTION DESCRIPTION DATA
    -- USER ID
    -- PORTAL ID
    -- CURRENT OOD IDENTIFICATION
    -- LOGICAL CONFIGURATION INVOKED
    -- PORTAL USEAGE TIME
* TYPE I ERROR DATA
    -- DEVICE LEVEL SCORE PER DEVICE, EACH TRIAL
* RAW DATA EXTRACTED (FOR FUTURE PROCESSING)
    -- RAW FEATURE SET PER DEVICE, LAST TRIAL
    -- THRESHOLD SCORE IN EFFECT PER DEVICE
    -- OTHER DATA FROM PIV

2) EXIT GRANTED

* TRANSACTION DESCRIPTION
    -- USER ID
    -- PORTAL ID

3) EXIT/ENTRY DENIED

* TRANSACTION DESCRIPTION
    -- USER ID
    -- PORTAL ID
    -- REASON FOR DENIAL

SECTION 5

PERFORMANCE CONTROL ALGORITHM

A. GENERAL

The performance control algorithm outlined in Figure 5-1 monitors and maintains the Hybrid Entry Control System (ECS) performance. It produces the parameters required for the entry control functions at the HIU, in the form of an Order-of-the-Day (OOD). The algorithm is defined by its six major functions, five of which are performed by the host, the sixth - the Hybrid Algorithm - is performed in the Hybrid Interface Unit (HIU) in the portal.

Error data collection and storage is the first task. All raw data generated during the entry process is collected at the entry control point (ECP), transmitted to the host in real time and stored for further processing.

The raw data is examined and queried in a batch process conducted by the host. The actual score values (ASV) produced by the entrant at the PIV in the portal are accumulated for Type I error data generation. In addition, the raw feature files used for the entry decision, also originating from the portal, are transferred to the host and compared for each entrant to the reference feature files of the population. The result of those comparisons, Type II ASVs, are then accumulated for Type II error data compilation.

The batch processing also finds and traces the goats in the population. As the raw data is analyzed, any user whose Type I or Type II performance extends beyond a prescribed limit is

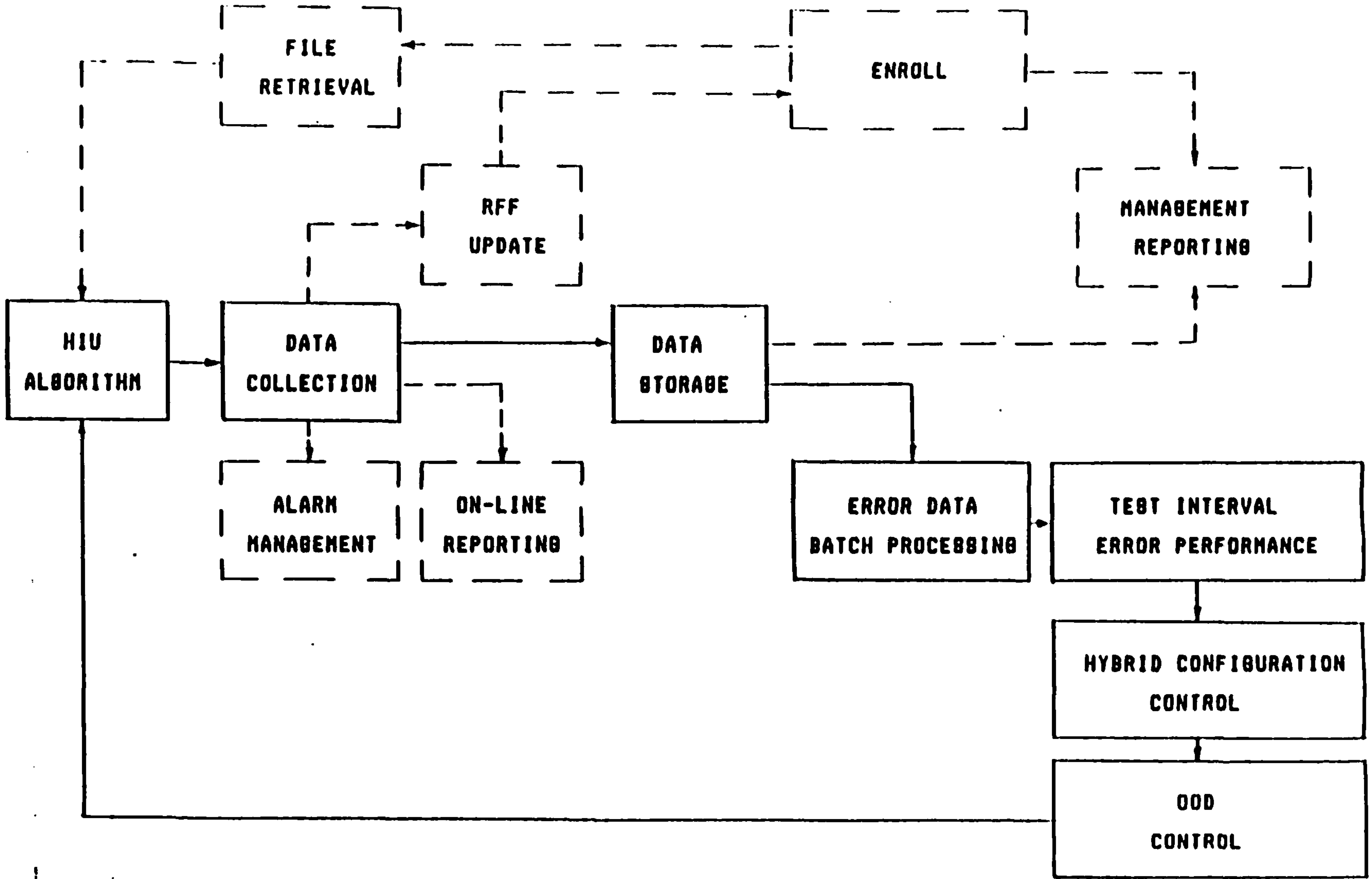


Figure 5-1: HYBRID ECS DATA PROCESSING; PERFOMANCE CONTROL ALGORITHM OVERVIEW (SOLID LINES)

flagged as a possible goat. Possible goats are then listed and individual performance statistics are accumulated for further processing.

Error data generated during batch processing is made applicable to a specified performance test interval. Acquired data is used to generate an error performance curve for each PIV that is a measure of how well the entire population performed on that device. From this true error performance curve (TPC), an operational performance curve (OPC) is generated for each device. This OPC is a subset of the TPC, the difference being those users defined to be actual goats, wherein all goats are removed from the set.

Upon definition of the actual goats, each user whose goat status has changed from the previous test interval must have his proficiency rating updated.

The next task is to upgrade the hybrid configuration control data. The operational test interval data is pooled with a known quantity of prior test interval data to generate a composite operational performance curve for the devices in the system. The composite OPCs are used to upgrade the elements of the logical configuration table (LCT).

The fifth of the performance control algorithm tasks required of the Host is that of generating an Order-of-the-Day table based on the newly updated Logical Configuration Tables. Base command data is also required to set hybrid-dependent factors used in producing the functional parameters the OOD table elements are to contain.

B. RAW DATA TRANSFER AND STORAGE

1. RAW DATA DEFINITION

The transaction record generated at the ECP and transmitted to the host is formatted so as to contain all the raw data required to permit performance control. The Type I raw data is in the form of actual score values (ASV), which are the direct result of the user raw feature files being compared in each PIV with the user reference feature file retrieved during the entry attempt. Type II raw data is the user raw feature file itself. Some configuration parameters are also required to be stored for the ensuing batch processing including the ID of the user, the threshold scores in effect during the entry attempt, the device level accept/reject decisions and each user's goat status.

2. DATA HANDLING

The C3P collects the transaction record, extracts the appropriate data required for performance control, and formats and stores the data in a chronological manner in a fairly large local buffer.

The Type II raw data for batch processing is stored separately from the Type I raw data, since an additional procedure is necessary to get the Type II raw data to the same process level (ASV) as the Type I raw data. The procedural flow is shown in Figure 5-2.

Required raw data file content is depicted in Table 5-1.

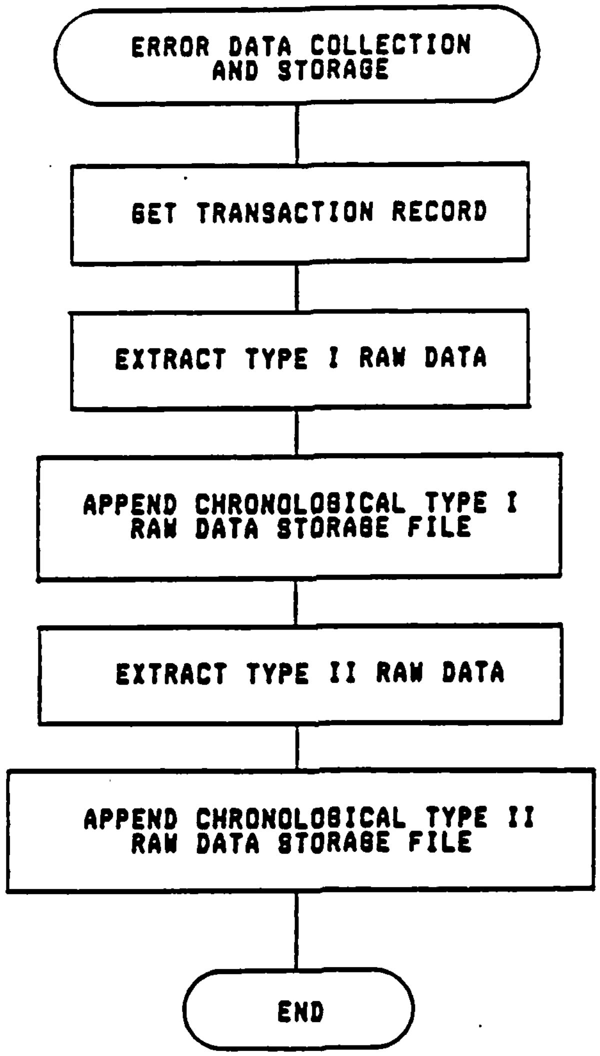


Figure 5-2: PERFORMANCE CONTROL ALGORITHM; ERROR DATA COLLECTION AND STORAGE

Table 5-1: RAW DATA STORAGE: FILE PACKAGE CONTENT	
TYPE I RAW DATA:	TYPE II RAW DATA:
* User ID	* User ID
* Device 1 ASV	* Device 1 Raw Feature File
* Device 1 A/R Decision	* Device 1 Threshold in Effect
* Device 2 ASV	* Device 2 Raw Featue File
* Device 2 A/R Decision	* Device 2 Threshold in Effect
* Device 3 ASV	* Device 3 Raw Feature File
* Device 3 A/R Decision	* Device 3 Threshold in Effect
* User Type I Goat Status	* User Type II Goat Status

C. ERROR DATA BATCH PROCESSING

Batch processing of error data produces useable empirical data in the form of score distribution curves (SDC) for each device type in the Hybrid ECS. The procedural flow chart is presented in Figure 5-3. Both Type I ASV, generated on-line at the ECP, and Type II ASV, generated during off-line processing, are reorganized into bins representing score distributions. Also generated during batch processing is a list of the possible goats - both Type I and Type II - for each type of PIV device. Criteria used to flag goats is described in the paragraphs "Type I Possible Goat Flagging".

The content of the files generated by the batch processing of the raw data is given in Table 5-2.

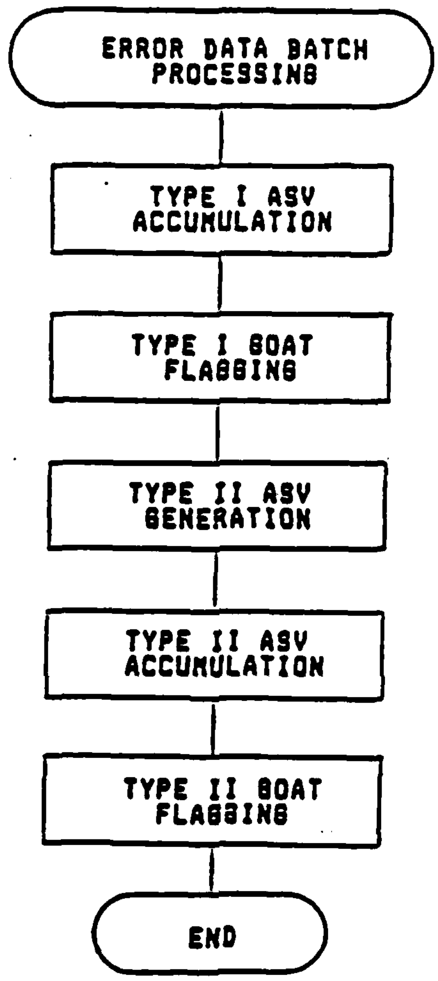


Figure 5-3: PERFORMANCE CONTROL ALGORITHM; ERROR DATA BATCH PROCESSING

Table 5-2: ERROR DATA BATCH PROCESSING RESULTS

Test Interval Accumulated Data (per Device, for TypeI/II)

* SDC (Frequency Distribution)
* Population Mean
* Population Variance
* Total Quantity of Scores Used

Possible Goat Lists (per Device, for Type I/II):

* User ID
* Total Scores Accumulated
* User Mean
* User Variance

1. TYPE I ASV ACCUMULATION

The EP, when not processing a higher priority task, retrieves the Type I raw data scores from its storage and accumulates them into an SDC for each device type. These SDCs are accumulated over a period of time, of pre-determined length, defined as the Test Interval, sufficiently long to give a reasonably precise representation of performance. The actual length of a test interval is based upon the size of the daily user population, and the precision required of the data produced during the test interval. A base with a large population will generate relatively accurate results in a short period of time. But as the user population becomes smaller, the test interval must be extended to gain the same.

As the SDCs are being accumulated by the batch process, the total quantity of ASVs, the average score of the sample and the variance of the distribution are maintained.

2. TYPE I POSSIBLE GOAT FLAGGING

In order for the Hybrid ECS to be more effective, goats are isolated from their respective PIV devices. The first step toward this end is flagging those users who could be goats. A possible Type I goat is defined as a user whose ASV history on any device is worse than the threshold score in effect when the ASV was generated. A device-level true-user rejection creates a possible Type I goat.

The first time any user is found to be a possible goat, his name is added to the possible goat list for that device, and a measure of his performance (mean and variance) on that device, updated. Once a user has been flagged as a possible type I goat, all ASVs generated by that user, on that device, on any ECP, are accumulated for the remainder of the test interval. This is required for two reasons; first, a realistic measure of his performance must be obtained for comparison with each of the other users on the same list, and secondly, unless all subsequent data is accumulated, not just the failures, the user will have no chance of being removed from the list.

The intention is to find those users whose performance on any device during the current test interval could adversely affect the performance of the system over the next test interval.

3. TYPE II ASV GENERATION AND ACCUMULATION

Before a Type II score distribution curve can be generated, Type II ASVs must be generated. This is accomplished by

comparing all raw feature files in the Type II raw data file package to the reference feature files in back-up storage in the EP. From this, the device Type II ASVs are accumulated in SDCs (with corresponding totals and distribution characteristics) in the same manner as the Type I.

This accumulation task is accomplished in the enrollment processor as a background function, in continual operation, unless a higher priority task requires the CPU. Type II raw data file package transmission (from C3P storage to EP temporary storage) occurs as requested by the EP, under suitable priority, over a dedicated transmission link.

4. TYPE II POSSIBLE GOAT FLAGGING

Type II goats are defined as those users whose reference feature files have the greatest chance of being matched by other users in the hybrid system. When the Type II ASVs are generated, the system will flag Type II goats when their reference feature file is responsible for an ASV worse than the threshold in effect when the raw feature file it was compared to was generated. Poor scores are noted for each PIV. Statistics are kept for each possible Type II goat in a consistent manner as with possible Type I goats.

D. TEST INTERVAL ERROR PERFORMANCE

Upon completion of the test interval period, the data accumulated by error data batch processing is further processed to gain a measure of the performance of the user population on each PIV device. This measured test interval error performance, with and without those users found to be actual goats, constrained within the precision of the operational performance data, is used to predict the performance of the PIV devices over the next test interval.

The procedural flow for this process is depicted in Figure 5-4.

1. TRUE ERROR PERFORMANCE OF PIV DEVICES

From each score distribution curve, a Type I and a Type II SDC for each device type, a true error performance curve is generated. These curves are desirable in order to show error probabilities of the PIV devices, were they to be removed from the hybrid environment. They also serve as the starting point for generation of the operational error performance curves.

2. ACTUAL GOAT DENOTATION

From the list of possible goats, Type I and Type II,per PIV device, those users who most seriously worsen the performance of the PIV device must be culled; these are defined as the actual goats.

First each list of possible goats is sorted. This sort is based on the statistics kept in the list. The keys used, and their relative merit are as follows:

... User score deviation; the closer the scores are grouped, the greater the effect removing that user will be. Tightly grouped poor scores have the greatest effect on the device's performance, if removed.

... User score mean; the poorer the mean score, the greater its effect on the population distribution (for Type I ; Type II is the opposite).

... Quantity of scores; Those users with the

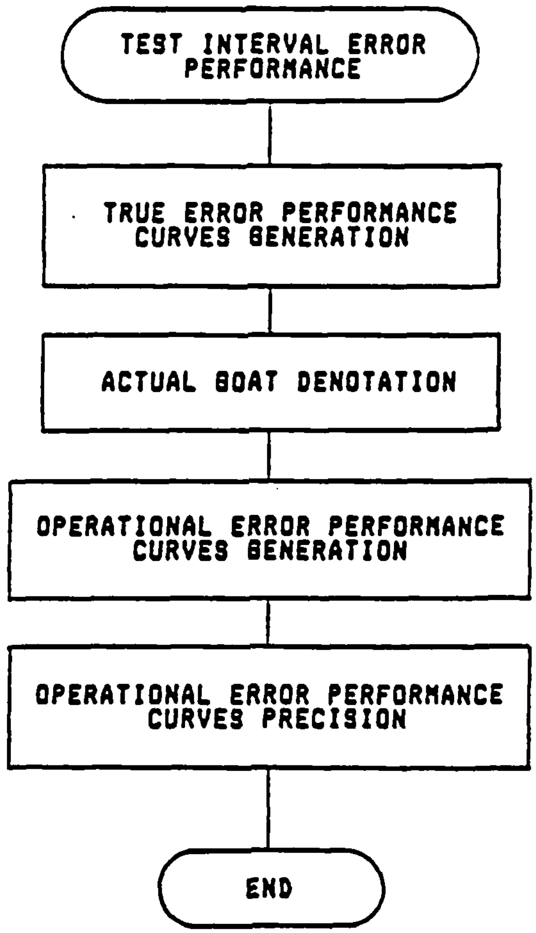


Figure 5-4: PERFORMANCE CONTROL ALGORITHM; TEST INTERVAL ERROR PERFORMANCE

largest quantity of poor scores will affect the distribution the most, all else constant.

... Time on the list; those users on the list the longest, can be labeled actual goats with more certainty, all else constant.

When all lists have been sorted, they are cross-checked for entries in multiple lists. No user is permitted to be a Type I or Type II goat on more than one device. A user can, however, be a Type I and Type II goat on the same device. If a user is found to be a goat on more than one device, he is kept on the list for the PIV in which he is a worse goat and removed from the others.

It is at this point that actual goat culling is accomplished. The intent is to isolate the ASVs of the worst offenders (those at the top of the possible goat lists) from the true population SDCs, until by removing the next user, the gain to the system operation will be less than the loss of usable throughput. Those users who are removed from the true SDC, are said to be the actual goats. The procedure for removing them is defined in the paragraphs "Limiting the Quantity of Actual Goats".

It should be noted here, that, once a user is denoted an actual goat on a device, statistics will be kept on him throughout the next test interval. That is, the actual goat list for the current test interval is the initial possible goat list for the next test interval and so on. The only way for a user to get off the actual goat list is to be replaced by another user defined to be a worse goat.

3. OPERATIONAL PERFORMANCE OF PIV DEVICES

The hybrid environment requires a Type I and Type II error performance curve for each device type, based on all users in the system who have not been denoted actual goats. This is the device operational performance curve (OPC). These curves are used to choose the threshold scores that will produce the device level error probabilities during system operation. The OPCs are generated by removing the possible goats (at this point they are now actual goats) until the functional limitation is reached whereby no relative gain is achieved by removing the next possible goat.

4. LIMITING THE QUANTITY OF ACTUAL GOATS

The true SDC has a known mean and variance calculated over the current test interval. Each user on the sorted possible goat list also has a known mean and variance. Starting at the beginning of the list, after each subsequent user has his individual score distribution removed from the true population score distribution, a new variance can be calculated for the revised population distribution. At the point when the change in the variance of the newly generated true score distibution is less than the precision with which the operational curve that will be generated from that distribution, the current distribution is said to be the operational score distribution. Those users culled from the possible goat list (whose personal distributions were removed from the population) are said to be the actual goats.

5. PRECISION OF TEST INTERVAL OPC

The precision of each OPC resulting from the test interval error performance procedure must be known. Each class (range of

scores, the center being a threshold score) and its corresponding error probability will have a known precision based on a given level of confidence. This is required for generating the composite OPC used in LCT element control.

E. HYBRID CONFIGURATION CONTROL

When the test interval device level error performance is known, system level error probabilities can be generated. The Hybrid ECS environment requires the OPCs for each device, from which the device thresholds and corresponding device level error probabilities are found, to be combined in a logical manner. These hybrid configurations are tabulated in the form of a logical configuration table (LCT), comprised of multiple elements, each defining the system errors attainable for the given configuration.

The procedural steps involved are depicted in Figure 5-5.

1. COMPOSITE OPC GENERATION

Upon completion of each test interval, device level OPCs are generated which define the error performance of each device during that test interval. A composite OPC is then generated with a large degree of precision, that predicts the error performance to be expected over the next test interval.

The composite OPC (for each device) is generated by pooling the current test interval SDC with some quantity of the most recently generated prior test interval SDCs. The exact number of SDCs to be used is given by the precision available when the pooling is to be done.

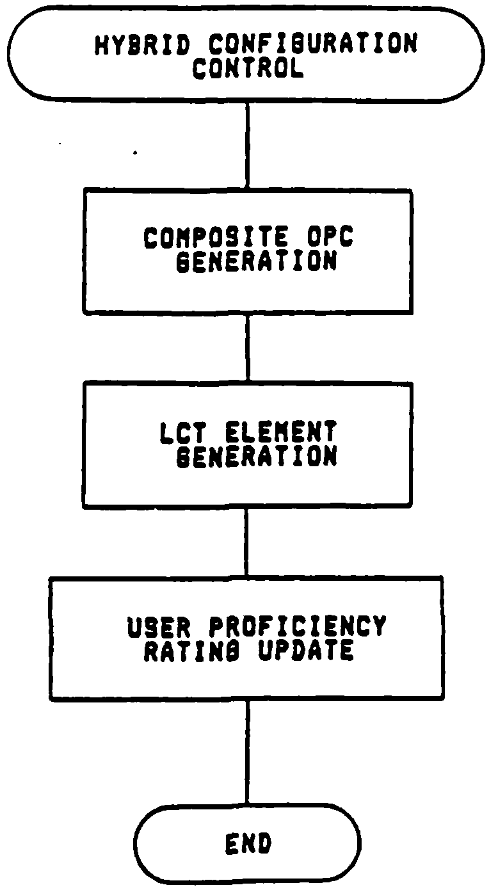


Figure 5-5: PERFORMANCE CONTROL ALGORITHM; HYBRID CONFIGURATION CONTROL

2. LOGICAL CONFIGURATION TABLE ELEMENT GENERATION

When the composite OPCs are generated for each device, the LCT elements can be upgraded. One element is defined for each logical configuration of devices, of which 27 exist, for example, in a three-device hybrid environment.

Each LCT element contains the system errors (Alpha and Beta total) that will occur if the device threshold values given are employed at the time of identity verification.

The LCT elements, therefore, can be used to know the required threshold settings to force a given system error probability, under any device logical configuration.

3. UPDATING THE USER PROFICIENCY RATINGS

A major task required of the hybrid ECS is to trace those users denoted as goats. The proficiency rating of each user makes this possible. The proficiency rating (PR) lists the PIV's in their ascending order of capability that the user has demonstrated on these devices. In addition, the user's current Type I and Type II goat status on any PIV is carried in the proficiency rating. A user PR is updated after each current test interval is completed if his proficiency on any device changes relative to another device, or if his goat status is to be revised.

F. ORDER OF THE DAY CONTROL

An Order-of-the-day (OOD) table is continually available to the ECS operator and to the HIU in each portal. The table contains one element for each of the possible required commanded levels of security. Included in each element is the priority and

contingency logical configurations (LC), for entry control point operations, and their corresponding values that will force the commanded system errors. The functional parameters required by the HIU and its algorithm (alarm disposition procedures, device fault procedures, device ordering requirements, etc.) are also included, and reflect the mode of operation for the entry control point.

The procedural flow for Host OOD control is depicted in Figure 5-6.

1. COMMANDED SYSTEM ERRORS

Each element of the OOD table is generated based on a commanded system error level desired to be in effect at the entry control point. For example, a scenario for tight security, requiring a relatively small system Type II error probability - and requiring a correspondingly higher Type I error probability - will be defined by one of the OOD table elements. The opposite of this - fewer Type I errors and relatively high Type II error probabilities - will be defined as another element of the OOD table.

Formatting such a table gives the Base Commander capability to put the hybrid ECS into the mode of operation required - at any time - quickly and effectively. Every scenario could be covered by one of the elements in the OOD table.

2. LOGICAL CONFIGURATION DATA

When the commanded system errors are known for each OOD element, the logical configurations capable of producing those errors must be found. Each element of the LCT is searched for an entry that will force the commanded errors. That entry is then

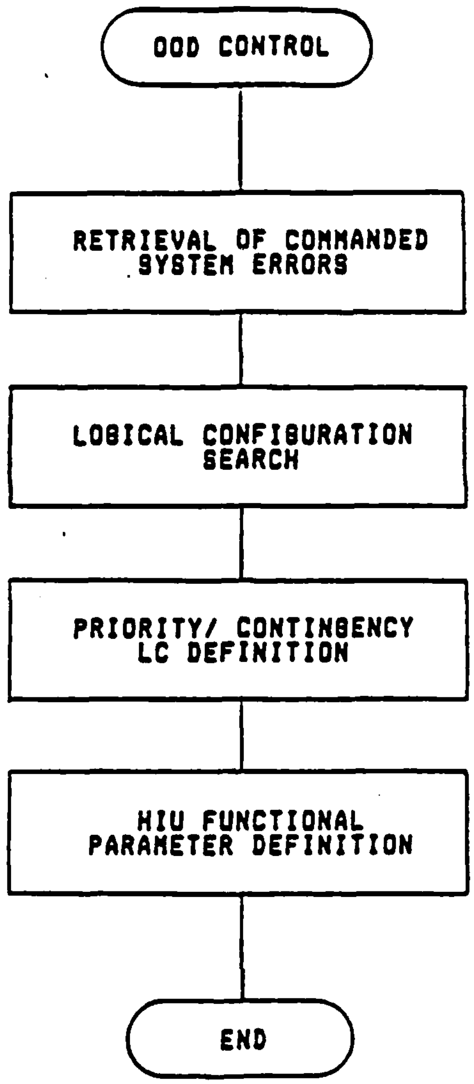


Figure 5-6: PERFORMANCE CONTROL ALGORITHM; ODD CONTROL

noted as to the exact errors and corresponding values. Of those configurations found to be capable of producing the commanded system errors, one is chosen to be the priority LC. The others will be sorted to serve as contingency LCs.

3. FUNCTIONAL PARAMETERS REQUIRED BY THE HIU

The OOD must define for the HIU all the procedural options that are under its command, in the form of functional parameters. The variables affecting the hybrid ECS operation and carried as parameters in the OOD table include:

* Alarm condition overrides; the HIU is equipped to handle all alarm conditions as a default situation. This parameter may define a course of action different from the default.

* Device sequencing; the HIU defaults to a device sequence at each entry attempt unless otherwise commanded.

* Raw data collection; the HIU defaults to a total collection mode unless otherwise commanded.

* Entry decision; the HIU makes the system entry decision, and controls the criteria for door locking/unlocking operations unless otherwise commanded.

* Status override; the HIU requires operational status condition reports of each of its constituents at a pre-determined interval. This parameter may alter the

interval between status checks and/or the reporting interval from th HIU to the host.

* Device degradation; the HIU is prepared to report on the the degradation stage of each PIV device when this parameter is commanded.

SECTION 6

HOST COMPUTER CONCEPTS

A. GENERAL

The concept for a distributed system performing the variety of tasks within the overall host computer is shown in Figure 6-1. The concept is built around the desire to provide support to the Central Security Officer while keeping the waiting time at any gate to an absolute minimum and while preserving the independence and the isolation of the identification files. It is desirable to offload each processor from those tasks foreign to its function, to separate and allocate the time-consuming tasks among a multiplicity of microprocessors and busses to obtain best overall throughput and bus security in the system.

Figure 6-1 shows the three principal functions to be performed in the host. A guard monitors consoles and printers to observe readouts and to give commands, aided by clerical personnel as required. A printer supplies hard copy and reports. Guard functions associated with Entry Control, described in Section 8, are tied closely with other functions associated with Intrusion Detection and Perimeter Security.

B. OVERALL SYSTEM

The C3 Processor in Figure 6-2 is normally involved in maintaining, on line, personnel logs and authorization files, time zones, alarms, base maps, base orders-of-the-day, transaction recordings, and reports. Its disks provide current personnel status and transaction history. It is tied to all portals via the ICPs and the C3 bus and its disks are accessed as required to buffer raw data from portals. It is tied to the

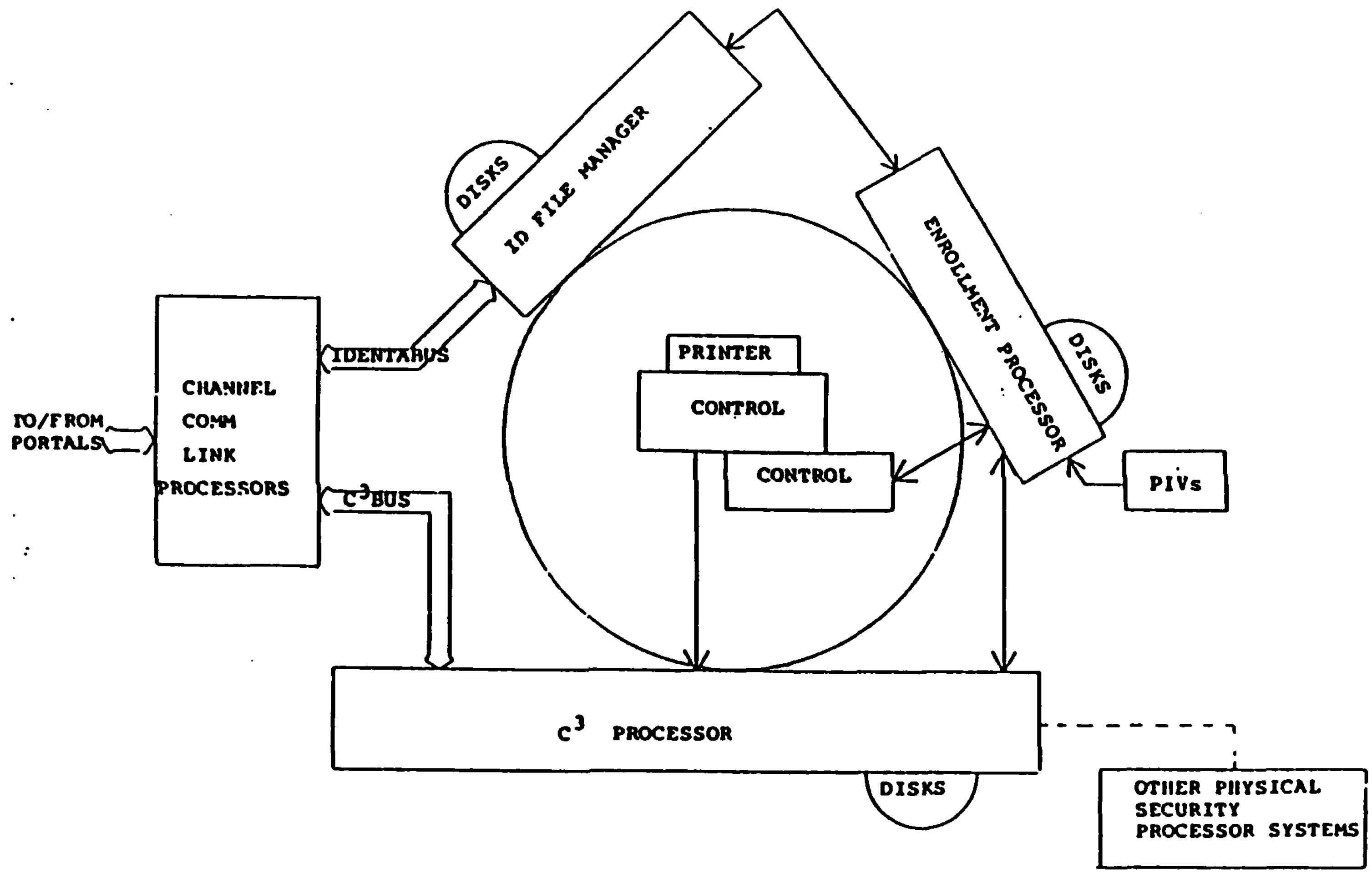


Figure 6- : ELEMENTS OF THE DISTRIBUTED HOST COMPUTER

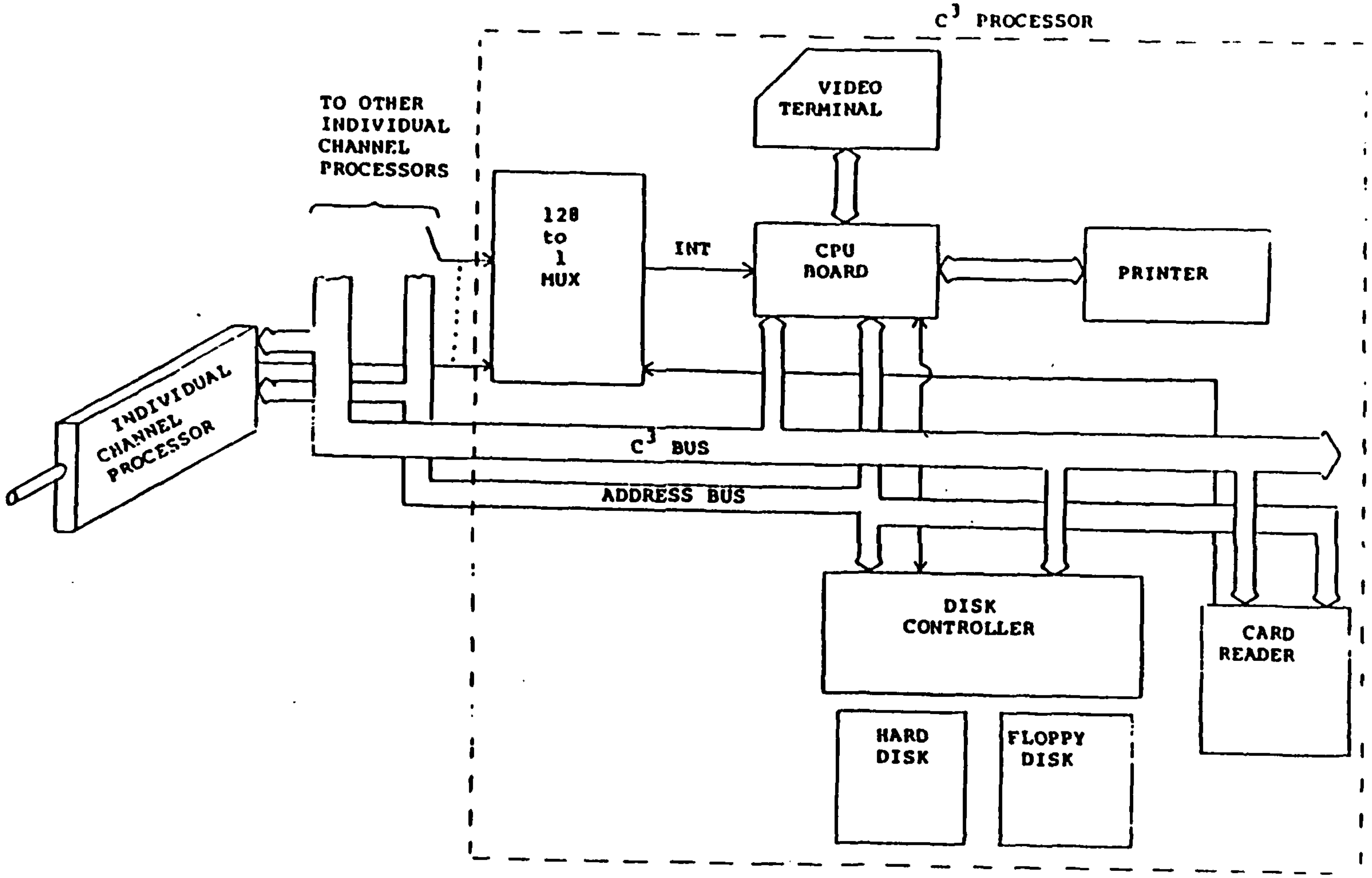


Figure 6-2: C3 PROCESSOR CONFIGURATION

Enrollment processor and transmits raw data periodically to that unit for batch processing analysis and performance monitoring purposes.

The Enrollment Processor is a batch operation device, generating identification files to be used for reference during matching. File-worthy data from each type of PIA device is processed to create the reference files, install them on hard-disk, and convert to tape for archival storage in Master form. A consolidated file of all features under one file name is considered to be best for use in a hybrid system, for throughput reasons. Typically the enrollment files are compiled in a time-sequential fashion and are transferred to working disks either immediately or periodically, as desired. Once enrolled, an individual's file is not deleted, but may have its number changed, or may be made inactive. A crossreference to a book of file numbers/names/service numbers, etc., is maintained clerically. Access to the files and to the enrollment function is closely guarded and controlled to prevent encroachment by imposters.

The ID File Manager, the IDENT processor in Figure 6-3, with its big disks, takes on requests for reference file retrieval and ships each file to its appropriate channel communication link processor using DMA techniques. Simultaneous requests from as many as 256 channels are arrayed in a calling sequence by the manager, to be handled as rapidly as the disk access mechanism can position itself, and read and disgorge the file.

C. RETRIEVAL TIME CONSIDERATIONS

Isolating the ID file retrieval function to its own distributed subsystem is a decision supported by the portal throughput timing diagram shown in Figure 4-3. Unless care is

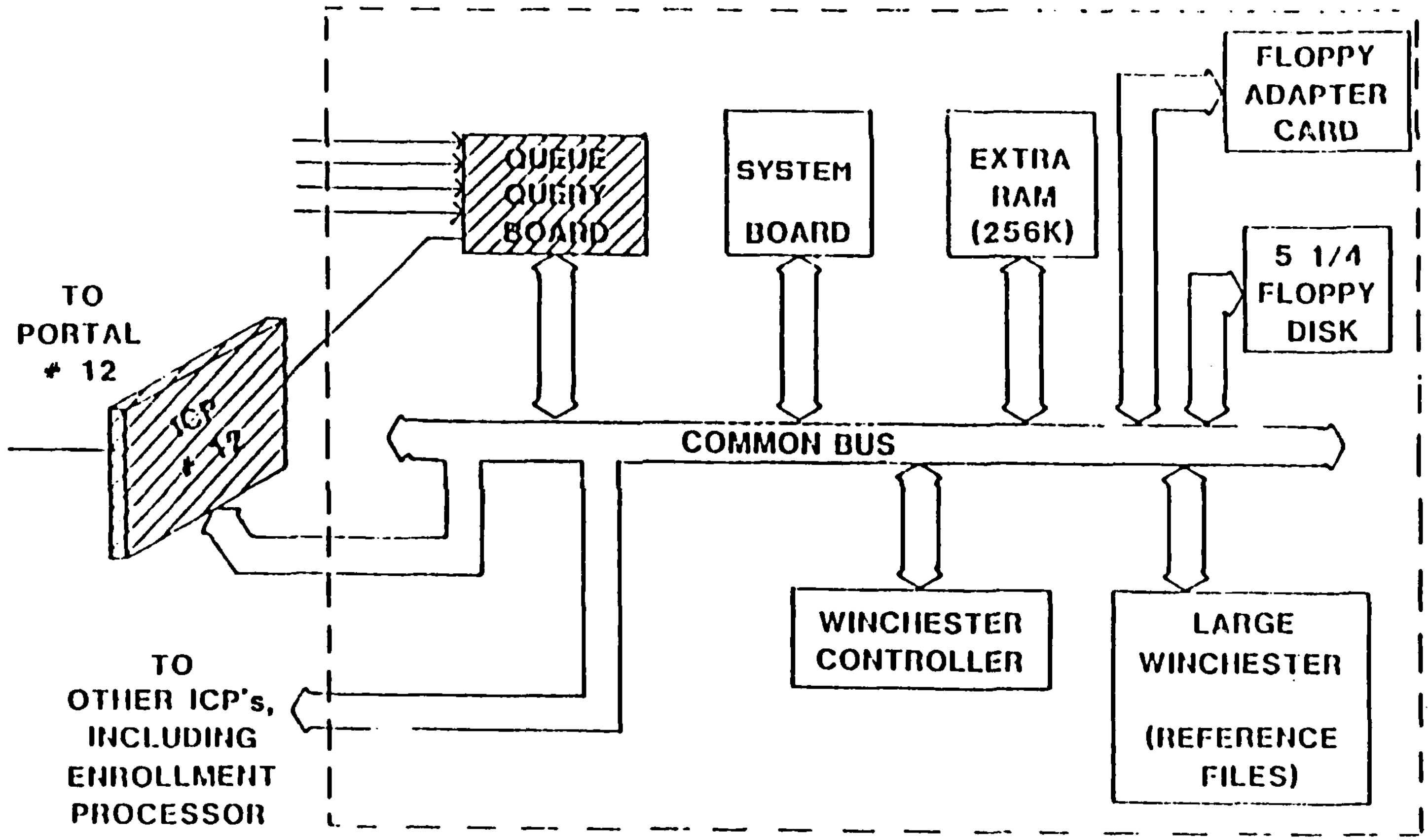


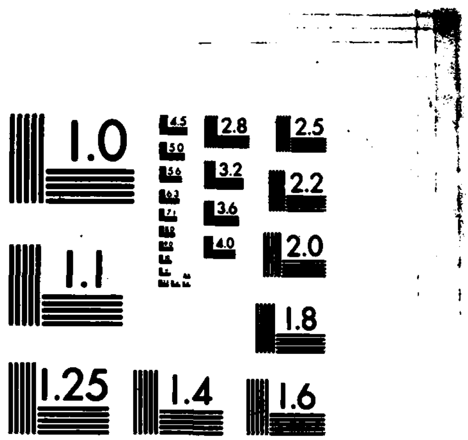
Figure 6-3: IDENT PROCESSOR CONFIGURATION

taken in the design, a major portion of the entry time is taken up by the wait time of the IDENT queue before the portal's channel can gain access to the file. In the peak load period, with typically 25 channels requesting service at once, a temporary queue builds, placing a premium on the IDENT processor's time. Unless specific design features are installed to correct it, with nominal disk access times of 100 milliseconds, a worst case wait on the order of 10 seconds can be expected, with a nominal in the 3 to 5 seconds range. Achieving minimum disk access time per portal and best overhead efficiency via DMA on the large reference file is one of the major design features required in the host system.

Off-loading the disk access processor from the time-consuming task of pumping the retrieved file through the communication channel to the portal is also a major design feature. Although this time is comingled with the inquiror's physical entry time and with his time to receive instructions and to address the PIVs, the data must nevertheless be at the portal prior to the completion of the feature scan in the first PIA device. Transmission of this reference file has been made, therefore, the task of an individual channel processor as was shown in Figure 4-6 rather than the disk access processor. The coercion toward this conclusion can be appreciated fully by examining Figure 6-4. Here, the baud rate at which data can be transmitted is constrained (at about 1200 bytes/second) by the line length, if a dedicated twisted pair is used, and constrained (at about 300 bytes/second) by telephone standards, if a telephone line is used. For file sizes between 1K and 20K bytes, using a single disk access processor to transmit to all 256 portals is not practical, creating peak load waits in excess of 80 seconds. Hence, parallel ICPs are included in the design concept.

AD-A147 922 HYBRID TECHNIQUES INVESTIGATION(U) SHANE-GELLING CO SEA 2/3
CLIFF NY D C SHANE ET AL. APR 84 SGR-84-01
RADC-TR-84-60 F30602-82-C-0167

UNCLASSIFIED F/G 17/2 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

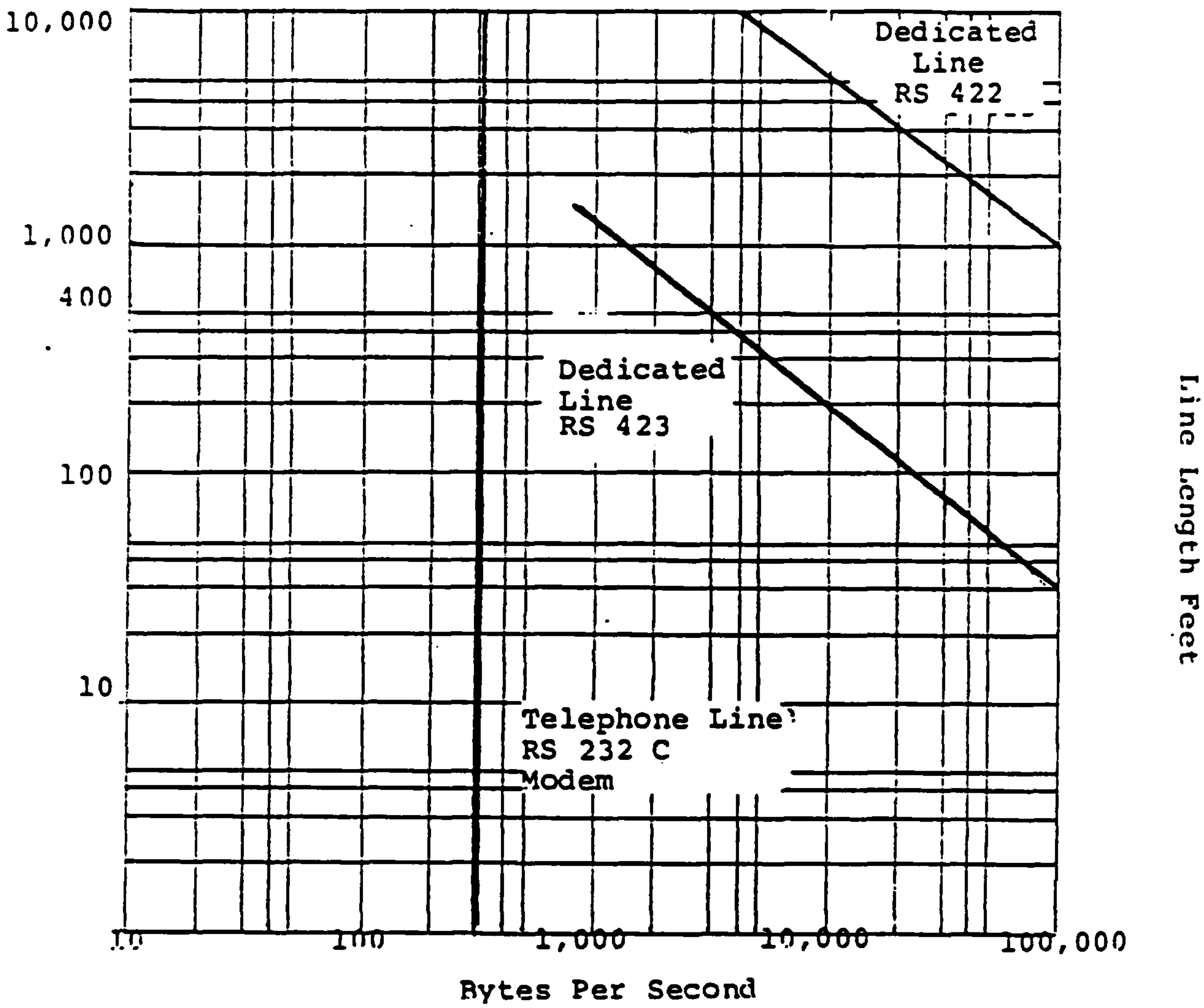


Figure 6-4: HOST/PORTAL TRANSMISSION SPEED LIMITATIONS

An individual channel processor is also desirable from the portal standpoint in order to permit data transmissions from the portal to be properly analyzed and directed to the appropriate functional subsystem comprising the Host. In effect, the C3 processor and the IDENT processor share the link to the portal, with the individual channel CPU as the arbiter. A listing of the functional transmissions between Host and the Hybrid Interface Unit at the portal is given in Table 6-1. Sharing does not cause a conflict for individual entry functions, because of their normal separation in time. Observance of protocol by the channel processor is required, however, to avoid interference between routine entry functions and the periodic batch process transmissions carried out over the link at any time during the day. This protocol is built into the logic on the individual channel board and into CPU software checkwords.

D. AUTHORIZATION DELAYS

A volatile file of persons authorized to enter any portal is carried in RAM at the portal. The file is updated periodically, via the communications link, from the main file in the enrollment processor via the C3 processor. Table 6-2 shows the format of each entry of this authorization table. This system architecture has been selected for two reasons:

1) additional time delay is avoided per entry since the C3 processor no longer has to handle authorization requests, but merely transaction recordings and verification responses. This reduces accesses on the C3 processor by at least 50%, and reduces delays in obtaining physical entry into the portals.

2) the opportunity is prevented that a would-be impostor might otherwise seize to overload the Host system by repeatedly requesting authorization to enter at some gate, via

TABLE 6-1	
FUNCTIONAL TRANSMISSIONS BETWEEN PORTAL AND HOST	
TRANSMISSIONS TO INTERFACE UNIT	TRANSMISSIONS TO HOST
* Order-of-the-day tables	* Request for file data
* Authorization tables	* Transaction results
* Time hack	* Alarm codes and data
* Override instructions	* Raw data
* Orders to the guard	* Maintenance messages
* Messages to the entrant	* Report data
* Reference file package	

TABLE 6-2

FORMAT OF AUTHORIZATION TABLE
-- EACH ENTRANT

Byte #	Character Designation
1, 2	Authorization Card Invisible Number
3, 4	User Reference Package Identification Number
5	Authorized Time Of Day For Claimed Identity
6	User Proficiency Number

card or key pad, and diverting the C3 processor from its normal tasks in servicing the other portals. The architecture not only limits the request by the impostor to the subject portal, but it denies an ID File retrieval attempt at the main file unless authorization is current at the portal, thereby protecting the efficiency of the main ID File retrieval process. The C3 processor, of course, must periodically refresh and rearrange each portal authorization file, but this is seen to be a background task, spread over a large time interval, not significantly impacting throughput.

E. ROUTING THE VERIFICATION SIGNAL TO C3

Another consideration towards minimizing time delays during entry is whether pulling the verification signal back to the host computer has value, compared to exercising the decision and its execution at the portal itself. Multiple interrupts to the C3 processor during any single entry attempt, which results if the Host is to decide, are to be dispensed with, if possible, since they act to place the portal at the end of the C3 queue with each interrupt, significantly holding up channel operation during the C3 queue time. Once the ID has been verified at the portal, an echoback signal from C3 seems pointless, since there appears to be no additional data at C3 to modify an entry-upon-verification decision at the portal which the portal can easily make.

Other instructions from the C3 processor to the Interface Unit at the portal are among those listed in Table 6-1. The instruction to enable the storage of the entrant's raw data file is intended to enter a series of checkwords into memory that, if present, causes the Interface Unit to execute that function. Other transmitted checkwords are used to cause status to be monitored on command from the guard's console acting on behalf of the Base.

F. INDIVIDUAL CHANNEL PROCESSOR CONFIGURATION

The tradeoffs in the design of the Host Computer architecture in the area of the individual channel processor can be identified with the aid of Figure 4-5. On this single board unit, one per portal, a 20K shared static memory serves as an intercept repository for all to/from communications transiting the channel. The on-board CPU is both interrupt driven and monitor-operated from the fixed-program ROM. The CPU directs the movement of all traffic outgoing from the board as well as incoming traffic from the Interface Unit. However, traffic destined for the Interface Unit from the ID File or the C3 Processor enter the 20K static memory through internal bus capture prompted by those processors. Traffic protocol is loosely administered by the CPU with the aid of specific logic chips that perform conflict-free memory addressing and bus enablement/direction functions. Protocol is made easy by the inherently straightforward time-sequencing of the channel functions. Randomness comes only from C3, and safeguards are included to prevent interrupt or override of a higher priority channel function by C3.

In this configuration, both C3 and ID File processors can address up to 256 channels with both the address bus and the data bus. Other information relating to the ICP is described in Section 4.

G. IDENT PROCESSOR CONFIGURATION

The IDENT Processor controller must rapidly disgorge full file data to the channel memory if the disk access efficiency is to be maintained. The controller uses its Direct Memory Access capability to accomplish the transfer. The file number to be retrieved and the channel number had previously come from the

portal to the 20K memory and had been called by the IDENT Processor upon receipt of interrupt or after queueing wait, if any, past interrupt from the channel CPU. With the channel number as its port number, the controller DMA directs its file to the proper channel via the DMA address bus and the IDENT bus. Upon completing the transfer, the controller is able to receive the next file number and the channel to send it to, from the IDENT Processor queue list, and it is immediately ready for another file access and another DMA to the appropriate channel.

As shown in Figure 6-5, the IDENT bus and the IDENT address bus link the DMA and its local memory on the disk controller to each of the 256 channels. Block transfers begin when the CPU sets up the DMA controller with the destination channel number. When the 20K byte transfer is completed, the DMA device sends an interrupt to the CPU as a signal to service the next channel having priority on the queue list. DMA rates above 800K bytes/second can be expected, so that DMA transfer time per channel is less than 25 milliseconds.

As shown in Figure 6-5, the request for file retrieval comes to the IDENT processor board from a channel decoder board. The decoder accepts hard wired inputs from all channels and, via latches, holds each channel flagged high until a poll of all channels is completed under the direction of the CPU. If the interrogation shows a ready flag from any channel, the IDENT Processor CPU is interrupted, a service routine is executed to list the channel number, return from interrupt and complete the poll.

At the beginning of the disk access operation a call is made to the channel number via the IDENT address bus and the IDENT bus to read the file number being requested. With this technique there is no contention for the IDENT bus among the channels, and

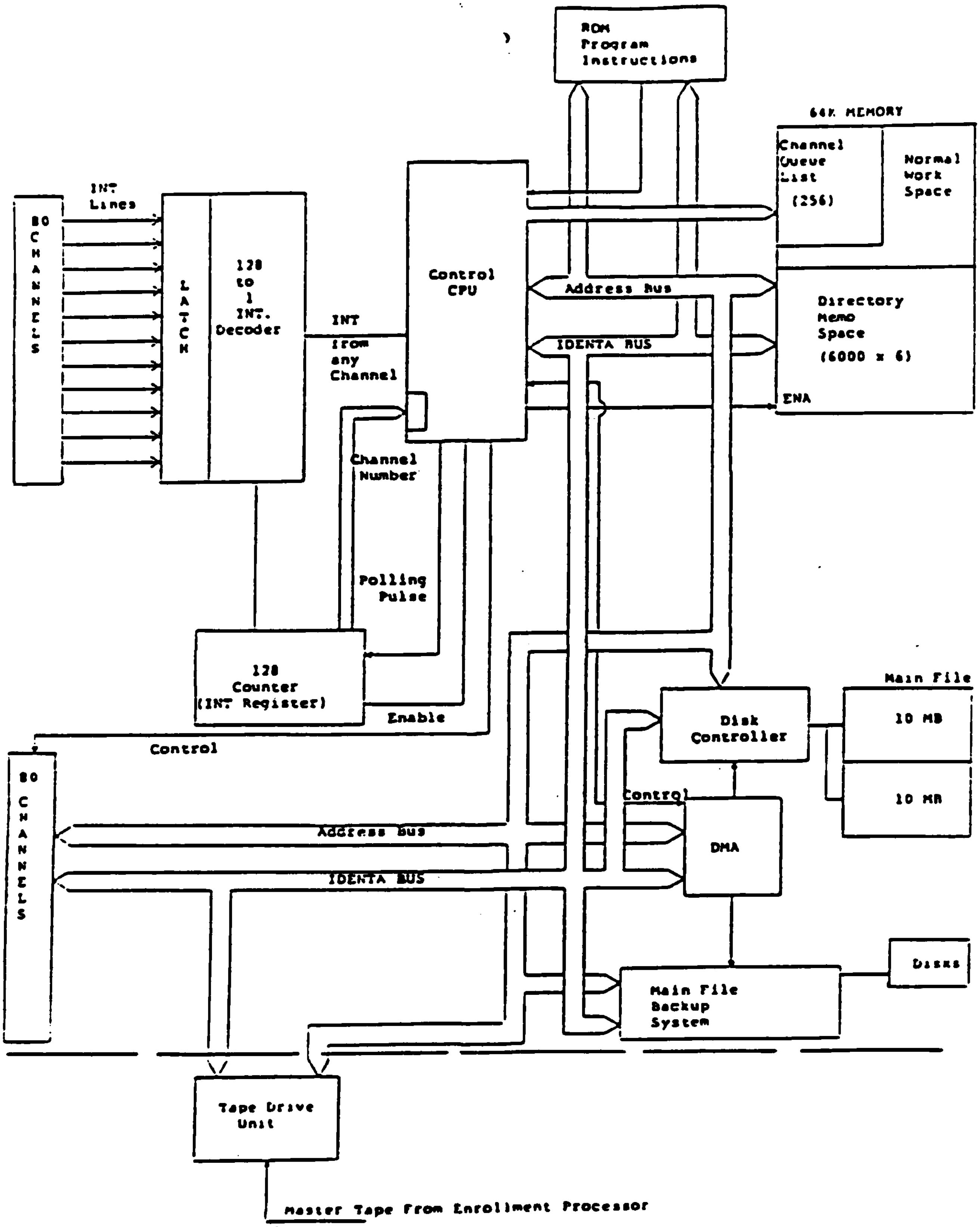


Figure 6-5: IDENT PROCESSOR CONFIGURATION

each is serviced with approximately equal priority.

H. DISK SELECTION

In the IDENT Processor design configuration, the importance of the selection of the type of disk and its attendant operating system software is evident. The recent advances in Winchester technology has permitted nearly order of magnitude reduction in costs for moderate size storage capacity, at relatively little loss in access time, but at much improved MTBF. Universal controllers are available for these disk drives, capable of running two or more drives from the single controller board. Hard disks are typically no larger than a floppy disk, typically within 4x6x10 inches. Their major drawback, inability to remove or replace the platter, does not seem to be a hindrance in this application, since the files, once established, are fairly stable in content, and file access is mainly for READ, with occasional WRITE operations. In this application, it is considered more cost effective to replace the entire disk than the platter, since by doing so, MTBF more than doubles, if the disk remains sealed from outside contamination.

Table 6-3 shows these Winchester disks to have a typical overall head positioning time around 50 milliseconds, mostly irreducible. Typical software drivers, however, of the general purpose type, are not as efficient in head positioning time as might be achieved with a special purpose driver, and new drivers are desirable with special purpose features to make best use of the DMA on the controller, if reasonably short queues are to be maintained.

This configuration takes advantage of low cost hard disks that are capable of storing the entire IDENT file of about 100 MBytes in a one or two disk set, and whose MTBF is at double the

TABLE 6-3 (1 of 4)
WINCHESTER DISK DRIVE CHARACTERISTICS

MANF/ MODEL	STORAGE (M BYTES)	TRACK FORMAT	BPI	ACCESS TIME (m sec)	TRANSFER RATE (M bits)	RPM	HEADS	ERRORS
MEMOREX 514	70	961	9912	45	5	3600	7	1×10^{-6} 1×10 1×10
MAXTOR XT 2140	110	1224	11,155	52	5	3600	15	1×10 1×10 1×10
MAXTOR XT 2085	70	1224	11,155	52	5	3600	11	1×10 1×10 1×10
PRIAM 503	71	755	9212	70	5	3600	7	1×10 1×10 1×10
PRIAM 505	111	755	9212	70	5	3600	11	1×10 1×10 1×10
VERTEX V170	57	987	9920	80	5	3600	7	1×10 1×10 1×10

TABLE 6-3 (2 of 4)
WINCHESTER DRIVES (con't)

MANF/ MODEL	STORAGE (M BYTES)	MTBF (HRS)	INT'FACE	DIMENSION HxWxL in.	DISK SIZE (i .)	POWER	COST
MEMOREX 514	70	11,000	5.25 STD	3.25 5.25 10.50	5.25	5V 2A 12V 1A	3400
MAXTOR XT 2140	110	11,000	ST 506	3.25 5.25 8.00	5.25	5V .7A 12V 1.37A	3675
MAXTOR XT 2085	70	11,000	ST 506	3.25 5.25 8.00	5.25	5V 1A 12V 1.37A	2630
PRIAM 503	71	10,000	PRIAM ANSI	3.25 5.25 8.00	5.25	5V 1.5A 12V 2A	2730
PRIAM 505	111	10,000	PRIAM ANSI	3.25 5.25 8.00	5.25	5V 1.5A 12V 2A	3590
VERTEX V170	57	11,000	ST 506	3.25 5.25 8.00	5.25	5V 1A 12V 2A	2350

TABLE 6-3 (3 of 4)
CONTROLLER BOARDS FOR WINCHESTER DISK DRIVES

MANUFACT	MODEL	HOST INT'FACE	DISK INT'FACE	TRANSFER RATE (M BITS)	FORMAT-TING	SECTOR SIZE (BYTES)	SMART	DIAG
OMTI	20L	SASI	ST 506	1.5	YES	256	YES	YES
DTC	500 SERIES	SASI	ST 506	5	YES	256	YES	OPT
DTC	5150	IBM HOST ADAPTER	ST 506	5	YES	256	YES	YES
XEBEC	S1410	SASI	ST 506	1	YES	256	YES	YES
SYSGEN	2100 2200	SASI	ST 506	1	YES	256	YES	YES
ADAPTIVE DATA	P SERIES	IBM PC	ST 506	5	YES	512	YES	YES

TABLE 6-3 (4 of 4)
CONTROLLER BOARDS FOR WINCHESTERS (con't)

MANUFACT	MODEL	BUFFER	DMA	DRIVES SUPPORTED	DRIVE TYPE	OS	COST ($)
OMTI	20L	YES	YES	2	HARD DISK	SASI PROTOCOL	245
DTC	500 SERIES	YES	YES	2/4	5.25 HARD/FLOP	N/A	520
DTC	5150	YES	YES	2	5.25	DOS 2.0	430
XEBEC	S1410	YES	YES	1/2	5.25	DOS 1.1	295
SYSGEN	2100 2200	YES	YES	4	HARD DISK	DOS 1.1	1400
ADAPTIVE DATA	P SERIES	YES	YES	2	5.25	DOS 2.0	395

MTBF of cartridge o. multiple head disks. In a double disk configuration the failure of a disk becomes a soft failure, in that only a segment of the totality of entrants is disabled, and the entrants can be detoured to other portals until a replacement is brought on-line. With such low cost disks in place, each set containing the whole file, a low-cost backup is also maintained current, ready for immediate disconnect and reconnect in less than three minutes.

I. IDENT PROCESSOR SOFTWARE

Relatively few new routines are required to run the functions in this specialized processor. With available intelligent controllers like the Western Digital WD-1000, these routines are simple, so they are expected to fit within 8K of ROM. The routines are variations of current file management techniques and include:

1. Queue list monitor:

While idling, the CPU is continually scanning the Queue list in RAM to determine if a channel interrupt has occurred, indicating a request for file retrieval.

2. File number collection:

Interrogates the interrupting channel to obtain the file number via IDENTABUS from COMMEM on the individual channel board.

3. Directory scan:

Each disk contains a permanent directory on Track zero which is brought out to the CPUs volatile memory at the time of booting. The directory is added-to randomly during the day, but

is sorted by ascending file number only once during the day, as a batch process. A scratch file holds interim file names until re-sort occurs. Each file name in the directory includes pointers to track number, head number and sector number of the files first record. All files are the same number of records in length. A file search system which finds the desired file name by sequentially splitting the file and comparing is expected to be the most efficient search technique. Since the directory is strictly ordered in RAM, isolating the file numbers in the matrix is not difficult. The scratch file is sufficiently small to permit sequentially comparing each number. Once located, the file number's associated head, track and sector numbers are commanded to the disk controller.

4. Disk Read/Write:

This is the disk driver. With a simple operating system (no frills) an intelligent controller, and an ordered file structure, this is primarily a standard 1/O execution to a standard port, with one or two variations, for selecting the data transfer area on Write, and for updating the directory on Write.

5. DMA:

A short program to move the file data from the disk controller's buffer to the individual channel's common memory (COMMEM) chips. Both of the memory buffers are larger than file size, so ratcheting via BUSY is not required, which simplifies this routine.

6. Directory Sort:

A periodic sort of the main file directory to add the latest enrollees, and bring the file up to date by setting its new scan

parameters. Also writes the resorted directory back on disk.

7. File Update:

Brings the IDENT files on new enrollees into the IDENT processor from EP processor and stores them on disk; updates the directory scratch file. The ID CPU also oversees a file update - e.g. a file renaming, or the addition of a new individual's feature vector from the enrollment subsystem.

8. Disk Diagnostics:

Consolidates the disk fault indication data, error completion codes, and DMA misses for transmission via the data link to the C3 processor for display and/or printout to the guard.

9. Disk Error Mapping:

Correlates file addressing on tracks and sectors with the plot of bad sectors on the disk obtained during formatting, in order to bypass those sector groups when laying down the files. Maintain this error map at the tail end of the directory file on disk and in RAM.

J. ENROLLMENT PROCESSOR CONFIGURATION

An isolated, centralized enrollment system has been selected as the most desirable. Centralized files in a double secure area with no outside access, identification of personnel required to operate the enrollment machines, isolated subsystem busses, operation audit trails, minimum opportunity for tampering, all point to the best security. A personal appearance of the enrollee at the enrollment station being a requirement, confirmation of

initial identity is straightforward, and identity correlation documentation can be established and maintained. An identity card number corresponding to the invisible number on the enrollee's card/badge, or his remembered number, if used, is entered clerically into the authorization records, based on personal appearance and upon personalized number assignment. Correspondence between invisible number and enrollee IDENT file number is also established at the time of personal appearance.

One or more copies of each of the types of PIV devices, as shown in Figure 6-6 are desired in the enrollment processor, possibly accompanied by a preprocessor. The PIV configuration is akin to that for any portal, that more than one unit may be required to give timeliness in enrollment or Type I/Type II batch processing. The units have the same Type I/Type II processing characteristics for raw data analysis as for enrollment analysis.

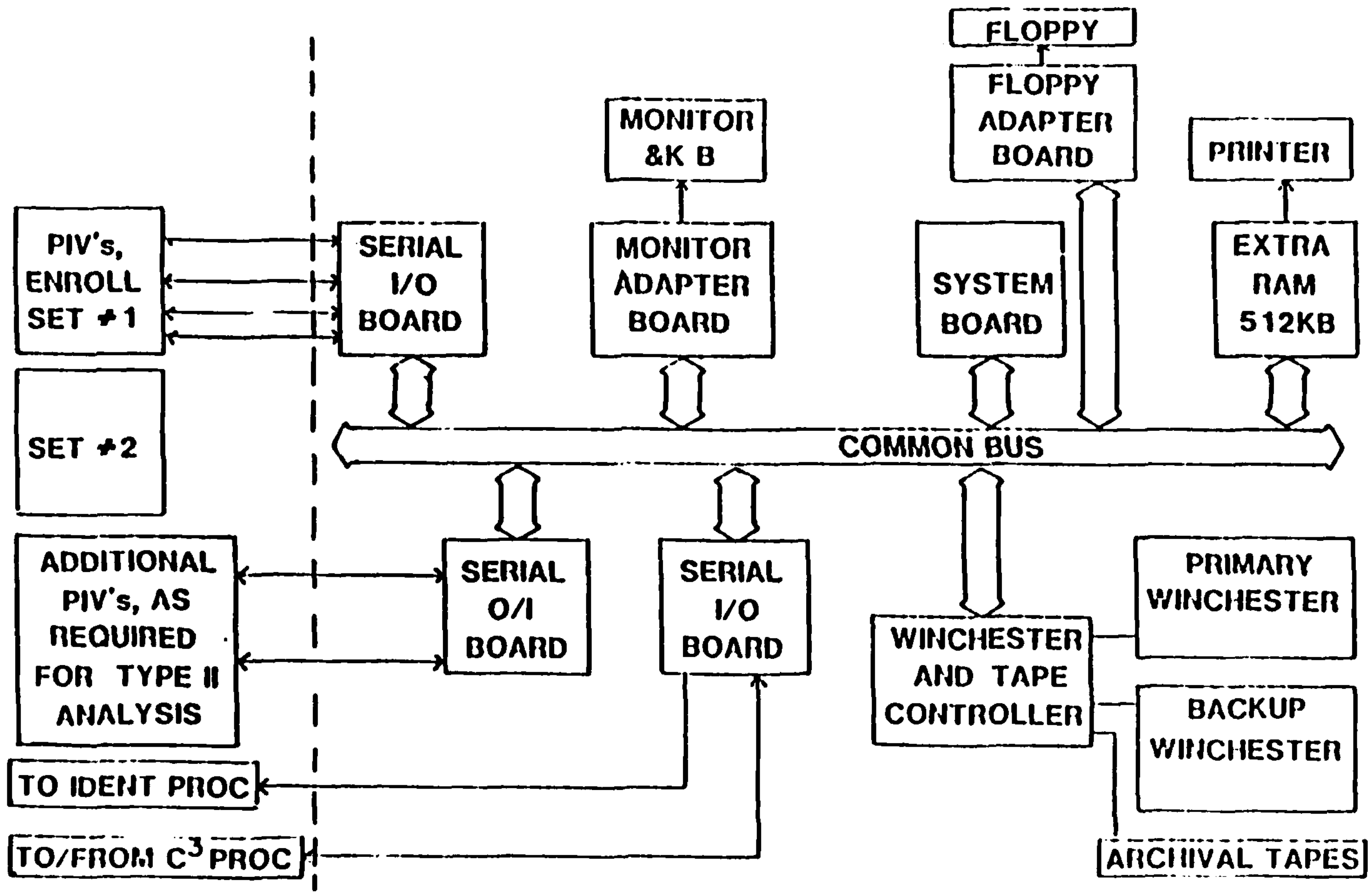


Figure 6-6: ENROLLMENT PROCESSOR CONFIGURATION

SECTION 7

ENROLLMENT CONCEPTS

A. USER ENROLLMENT

Incorporation of each user into the ECS file is accomplished primarily with the normal user initial enrollment, then secondarily a normal user re-enrollment and an administrative reference package update. The visitor/temporary enrollment procedure incorporates those users with limited file life. For purposes of description, an identity card and a PIN are presented to be used, rather than a remembered number only.

1. NORMAL USER INITIAL ENROLLMENT

A personal appearance at initial enrollment is necessary to provide a user reference file package (RFP) to the system. The reference file package is a multi-part file consisting of a descriptor record and the device reference feature files (RFF). The descriptor record is, for the most part, an administrative file containing the following data at a minimum.

a. Personnel Data
   1. Name
   2. SSN
   3. Ht/Wt/Eyes/Hair
   4. Age

b. Authorization Data
   1. Administrative Identification number of the card issued user at enrollment
   2. Invisible number of the card

3. PIN

c. Enrollment History Data
   1. Date/Time of all enrollment procedures
   2. Authorization/Title/Name/file number of enroller.

The authorization card data may be temporary at time of initial enrollment, but an update is allowed upon permanent card issuance.

The procedure, as shown in Figure 7-1, requires the data for the administrative portion of the descriptor record to precede the user, in conjunction with such items as security clearance.

The operator initiates the procedure at the keyboard in the enrollment processor. The personnel data is entered, preferably as responses to canned input requests. The administrative card identification is then entered and the card itself placed into a card reader for automatic retrieval of the invisible number. The personal identification number (PIN) is then encoded from the invisible number issued to the user, and added to the descriptor record.

At this time the user is instructed as to the operation of all portal equipment and requested to address each PIV device for reference feature file generation. The EP must create each file in turn, and must process multiple renditions, typically a quantity of five.

An abbreviated goat analysis of the user is performed to initialize a proficiency rating for each user. It is

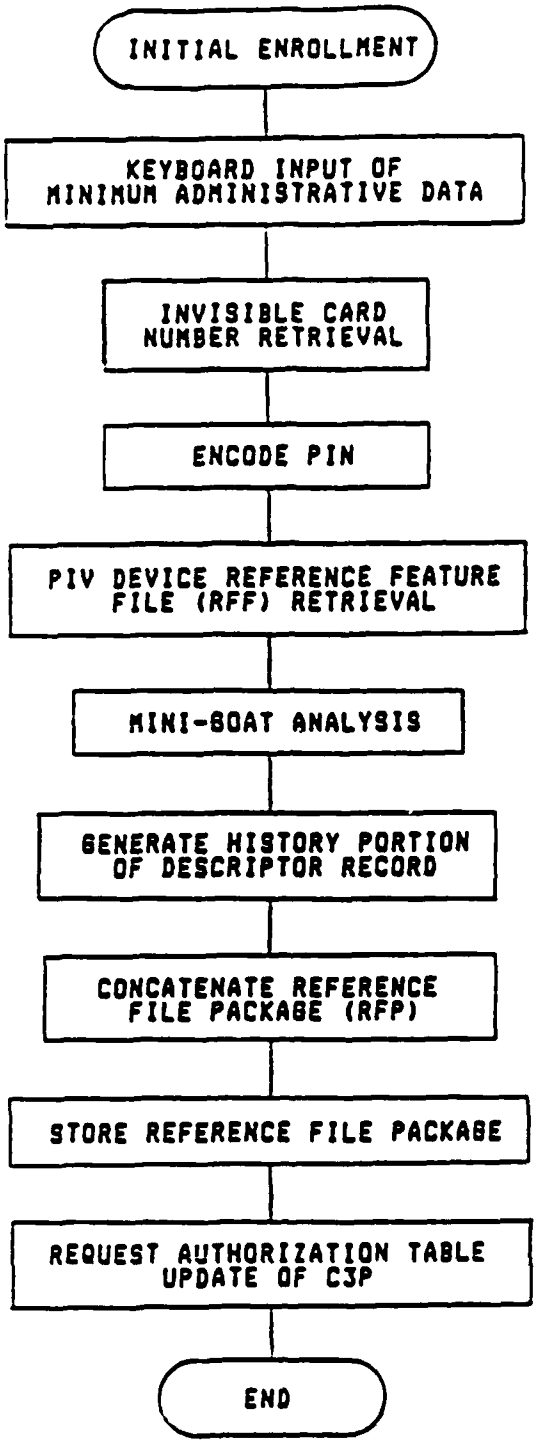


Figure 7-1: PROCEDURE FOR NORMAL USER ENROLLMENT

accomplished by comparing each reference feature file generated to the existing reference feature files of 20 other users, for each device category, to assess Type II goat potential. Type I goat status is preliminarily a result of analyzing the enrollment statistics transmitted by each PIV enrollment device, and comparing them to the other goats in the population statistics. The users relative ability on each device is also calculated, for Type I purposes.

At this point the descriptor record is completed, the reference package concatenated and titled by an encodement of the invisible number of the issued card. It is duplicated for storage in three places; archive, back-up, and IDENT. The disk directory of the back-up copy is sent with the copy for the IDENT for exact duplication storage.

An authorization table update request is then executed in order to permit this user's authorization data to be sent to the appropriate portals. The user ID (invisible number), user proficiency rating, user file name, and entry time codes with portal numbers are required to be added to the master authorization table in the Host.

2. NORMAL USER RE-ENROLLMENT

Re-enrollment is required if the initial enrollment process generated a reference feature file, on any device, not currently suitable, for any user. This procedure will allow only one device reference feature file to be altered. The result is an update of the existing reference file package for the user. This procedure must be authorized and carried out under the supervision of personnel in security central.

The operator initiates the procedure at the keyboard, and the EP then requires insertion of the users authorization card and PIN. This allows retrieval of the current reference file package in EP back-up storage.

The procedure for normal user re-enrollment is shown in Figure 7-2.

The user is instructed to address the PIV device from which a new reference feature file is to be retrieved, and the device is requested to proceed. Upon receipt of the newly generated reference feature file it is compared to the feature file from the current reference file package. It is here that a decision is to be made on the validity of the new reference feature file.

If the re-enrollment was required because the user is a Type II goat, a mini-goat analysis is carried out. If after a comparison with the existing statistics on the user (generated by batch processing), the goat status of the user is changed for the better, the procedure is said to be valid. Otherwise, a second try is in order. If the re-enrollment is intended for Type I purposes, the user is requested to address the machine for entry-equivalent tests. The goat status is generated and compared to the existing status, and a decision made on the validity of the re-enrollment. If the newly generated feature file is to be kept, the current reference feature file is updated.

In either case the enrollment history record is updated, and the revised reference file package stored in archive and EP back-up. The IDENT reference file package is altered only if the reference feature file is altered.

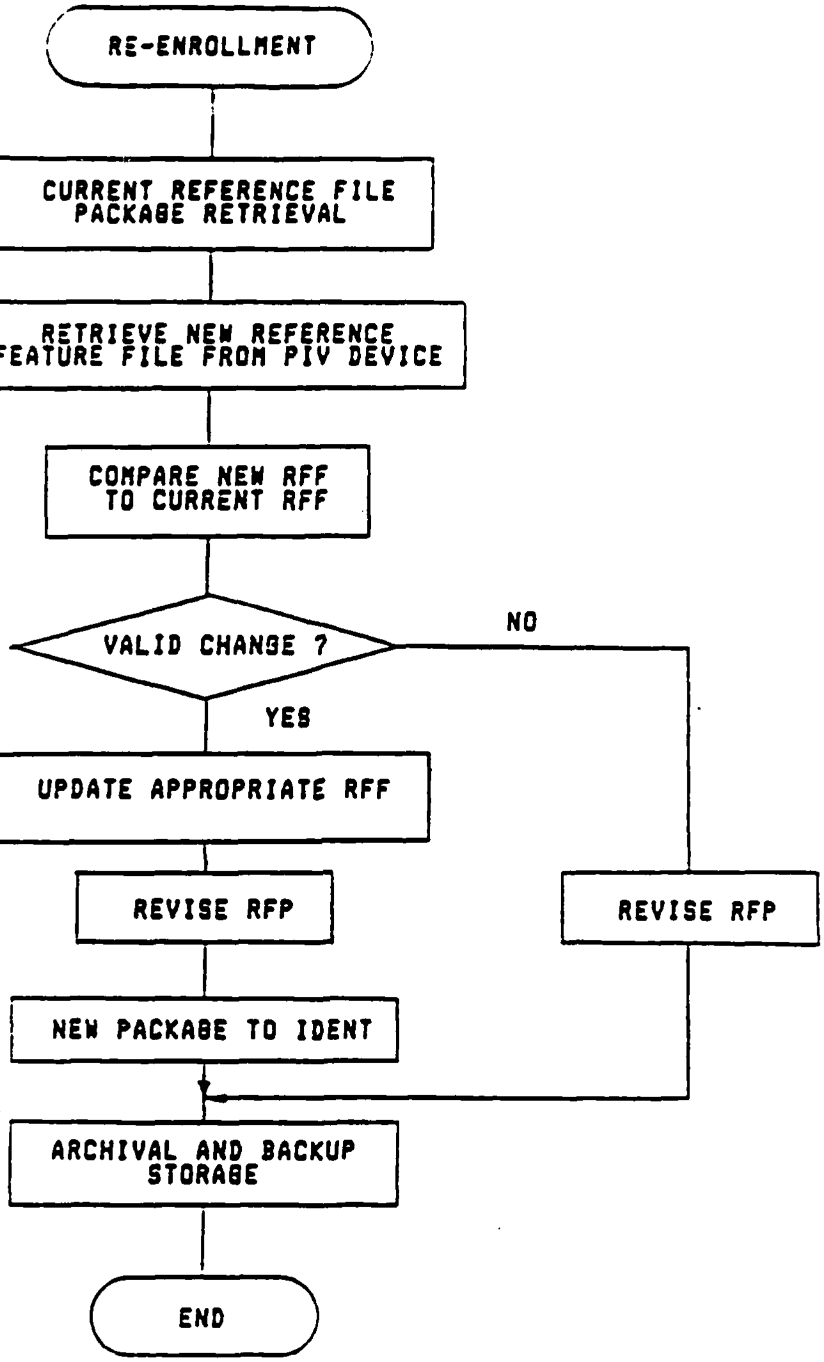


Figure 7-2: NORMAL USER RE-ENROLLMENT

3. ADMINISTRATIVE REFERENCE PACKAGE UPDATE

This procedure is capable of altering only that data contained in the descriptor record of the reference file package. No alteration can be done to the reference feature files using this procedure.

The operator initiates this procedure, shown in Figure 7-3, entering the current invisible number of the users authorization card (the user must be present) thereby retrieving the reference file package. Alteration can then be accomplished on the descriptor record. The enrollment history data will be appended, and if a new authorization card (and therefore new invisible number and PIN) is to be issued, the file is re-titled and rewritten to archival and back-up storage. A filename change is requested of the IDENT (if applicable), and the procedure ended.

4. VISITOR/TEMPORARY USER PROCEDURES

Even visitors and temporary card issuances undergo enrollment procedures.

Three categories of visitors have been defined: a) Transients: these visitors are treated like normal users by the system, and if no reference file package precedes them, the enrollment procedure is the same. The transient's reference file package, however, is given only a limited useful lifetime in the system. b) Temporary: these users have their reference file package precede them or their reference package is on file, and needs only to be re-activated. c) Escorted: this category has no reference feature files generated, but requires a certified escort recognized by the ECS, in order to be processed through any portal.

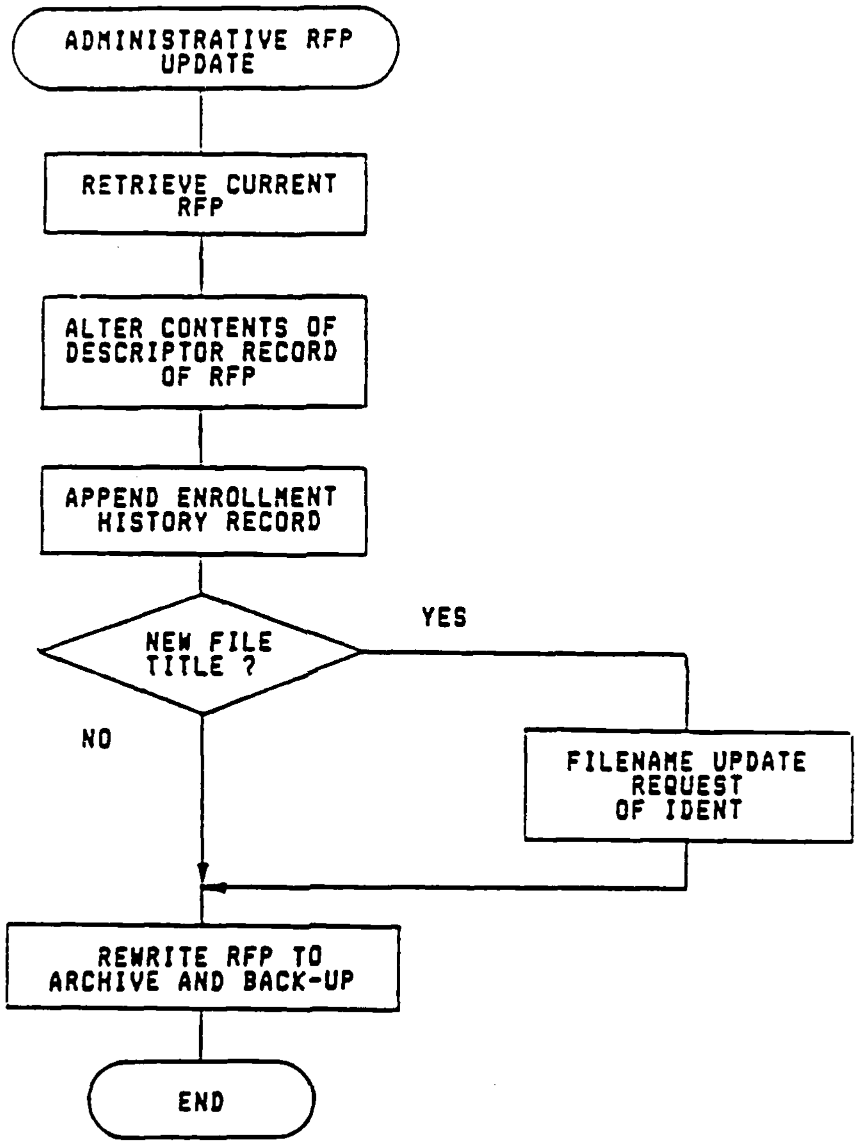


Figure 7-3: ADMINISTATIVE REFERENCE PACKAGE UPDATE

Temporary card issuances are for those users, authorized in the system, who do not have their authorization card in their possession when system usage is required.

Transient users who have an existing reference file package need not undertake full enrollment, but can be verified as a part of the transient enrollment procedure. If no file is available, the enrollment procedure is the same as for normal initial enrollment.

The transient enrollment process requires the user to address each PIV device, as if an entry attempt were being made. The EP will retrieve the file, as well as receive the raw data generated in the PIV. On devices that require it, the reference feature files will be updated, and an abbreviated goat analysis will generate a proficiency rating for the transient.

If required, a new valid authorization card and PIN is issued, and the descriptor record is updated. The reference file package is updated and stored as in normal enrollment and the C3P is requested to update the master authorization file.

This procedure is shown in Figure 7-4.

A user classified as a temporary does not need to be newly introduced during the re-enrollment action. The operator will add the reference file package that precedes the user, or reactivate an existing one to the system.

The operator must update any descriptor record data. The EP will append the enrollment history, store the file and request authorization update via the C3P.

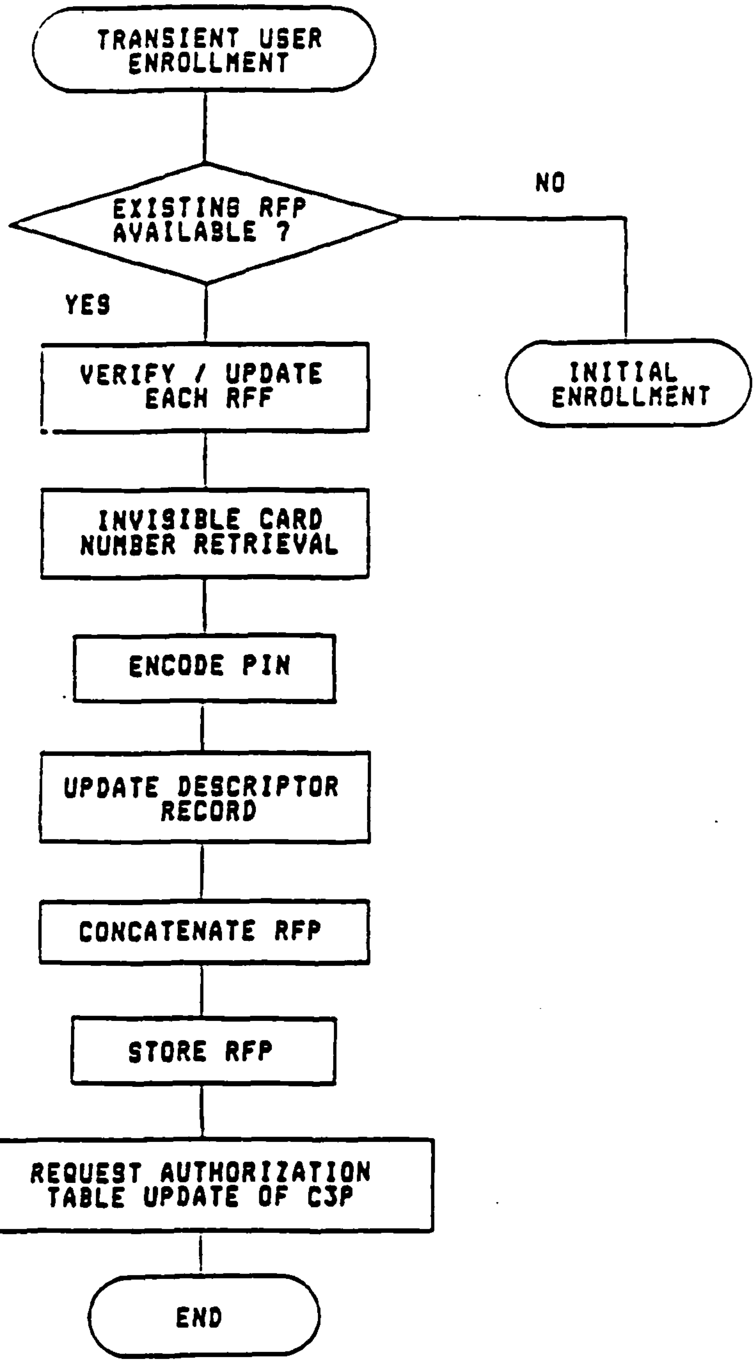


Figure 7-4: ENROLLMENT PROCEDURE FOR TRANSIENT VISITORS

The user must be present to receive the temporary card, and to confirm his identity with the card. This procedure is shown in Figure 7-5.

Any user classified as an escorted visitor has no requirement for reference feature file extraction. The operator at the EP enters the minimum required administrative data via the keyboard, with the designated escort ID an additionally required input. The valid authorization card to be issued is read by the card reader at the EP, and the invisible number extracted.

For escorted visitors a PIN is required. This is a five digit number, the first of which is a number used exclusively for visitors. The last four may coincide with the last four digits of the users social security number, or equivalent.

The reference "package" - in this case, only a descriptor record - is stored. A request for master authorization table update is made via the C3P.

This procedure is shown in Figure 7-6.

When a user requires entrance via the ECS, and does not have in his possession his authorization card, a temporary card can be issued, as shown in Figure 7-7.

The operator must retrieve the appropriate reference file package, the user must enter his PIN, and the temporary card can be issued. The enrollment history must be updated, and the file stored in archive and back-up.

For update to the master authorization table, the invisible numbers of the temporary and initially issued cards must accompany the request.

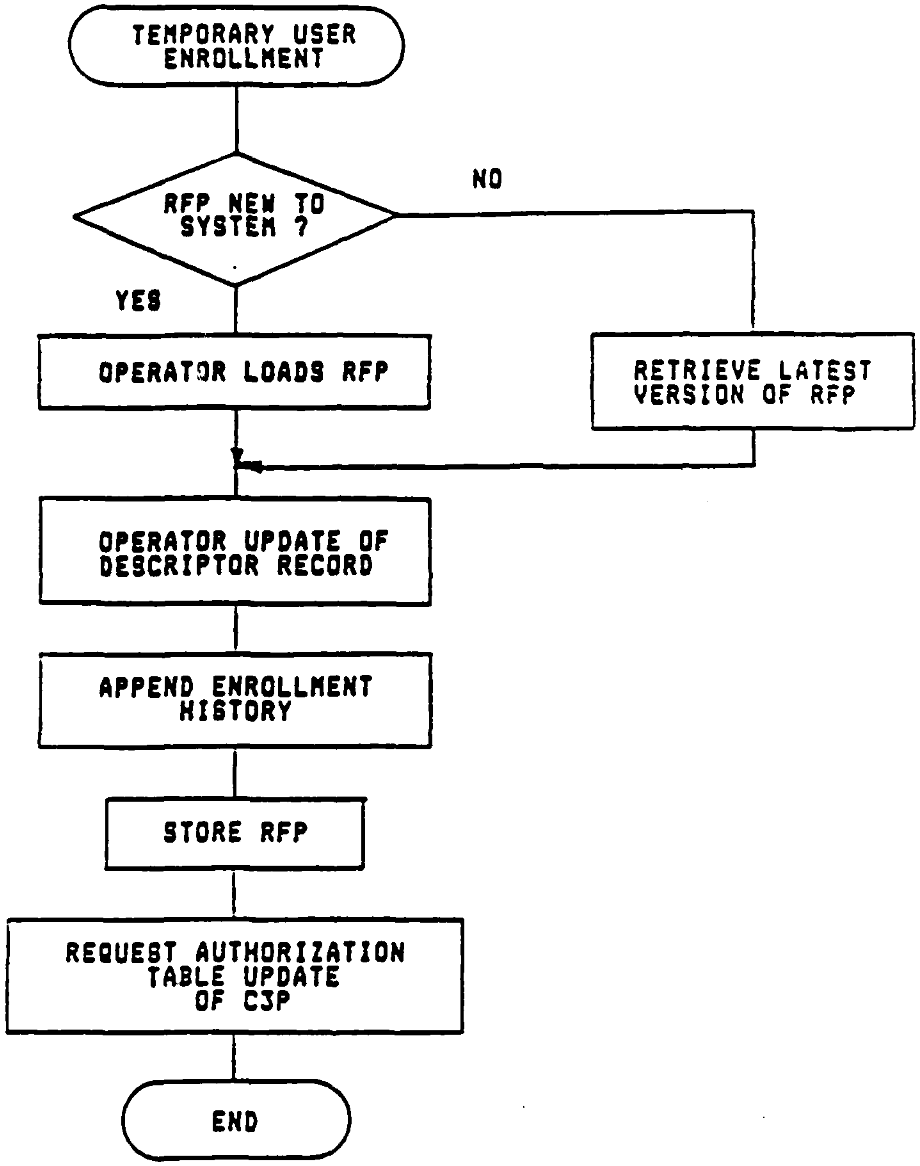


Figure 7-5: ENROLLMENT PROCEDURE FOR TEMPORARY VISITORS

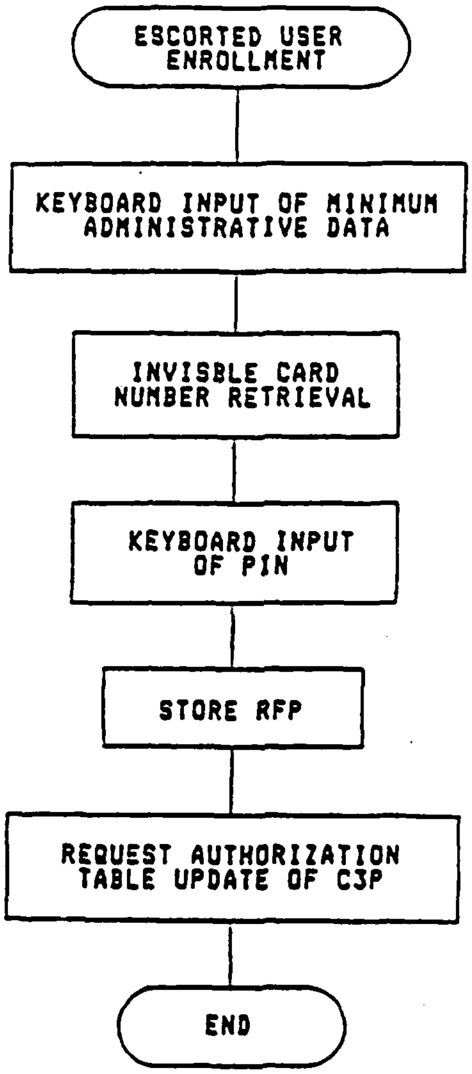


Figure 7-6: ENROLLMENT PROCEDURE FOR VISITORS REQUIRING AN ESCORT

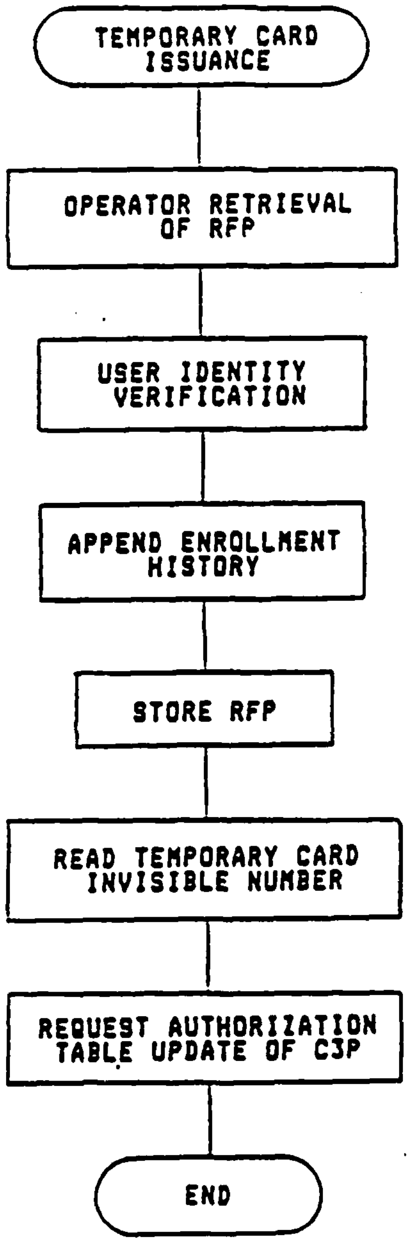


Figure 7-7: TEMPORARY CARD ISSUANCE PROCEDURE

5. DEENROLLMENT

Identity numbers for all persons no longer authorized are clerically entered as lockouts, and their numbers are removed from authorization tables at all portals. Reference files, however, are retained.

SECTION 8

GUARD FUNCTIONS IN A HYBRID SYSTEM

A. GENERAL

The man/machine interface between the conceived Hybrid Entry Control System and the Guard Force becomes considerably more sophisticated as the level of discrimination in the Hybrid increases. With the system error rates at better than one in 10,000 for both Type I and Type II, the quantity of Type I alarms in a mature base population of 5000 persons drops to around one per day. This event rate at a portal is thus so low, measured against current rates, that it becomes a sideline or background event. The role of the guard, therefore is shifted somewhat, from his current role of visually-stimulated decision-maker with a required high degree of vigilance, to that of an audibly-stimulated monitor, with a lower required sustained level of vigilance. This evolution is a step in the right direction, according to studies that show effectiveness dropping off if a high vigilance level is required. A guard is considerably more effective if he is occasionally stimulated to a hign level of required vigilance of short duration. The Hybrid System requires the guard to exhibit high levels of skill during occasional events, with high attention and diligence given to the task during the event period.

Within the Hybrid System, several distinctly separate roles are evident, primarily the result of the physical separation desired among the participating stations. These guard force activities take place 1) at the Portal, 2) at the Central Security Office, and 3) at the Enrollment center. To the extent that the physical separation requirement is eliminated, the roles

may merge. If vehicle entry control is to be included as a part of overall entry control, additional tasks are placed upon the guard. However, the role described herein is limited to his task of assisting the vehicle operator to verify that he is authorized to enter the station in question.

B. AT THE PORTAL

A typical Hybrid System Entry Control Point is shown in Figure 8-1. Five portals containing multiple PIV's are arranged in a manner inside a gatehouse designed to speed throughput. The entry to the gatehouse is under the surveilance of a guard in a booth with peripheral visibility throughout the gatehouse. Each portal has an optically clear material in its upper half, and all PIV's are at table level. Users must enter the gatehouse in the full view of the guard or guards, and any queueing would occur in front of the guard booth, before the user was sent to a soon-to-be empty portal. Detention booths are accessible from each portal so that a user rejection frees up the portal for the next user. With this layout, three interrogation stages can occur: 1) visual observation by the guard, 2) machine analysis by the PIV's in the Hybrid System, 3) verbal inquisition by Security Personnel on those users in detention.

The possible foreground events occupying a portal guard are:

1. disposition of visitors approaching the portal

2. disposition of authorized persons requesting temporary badges for entry at the portal

3. parcel inspection

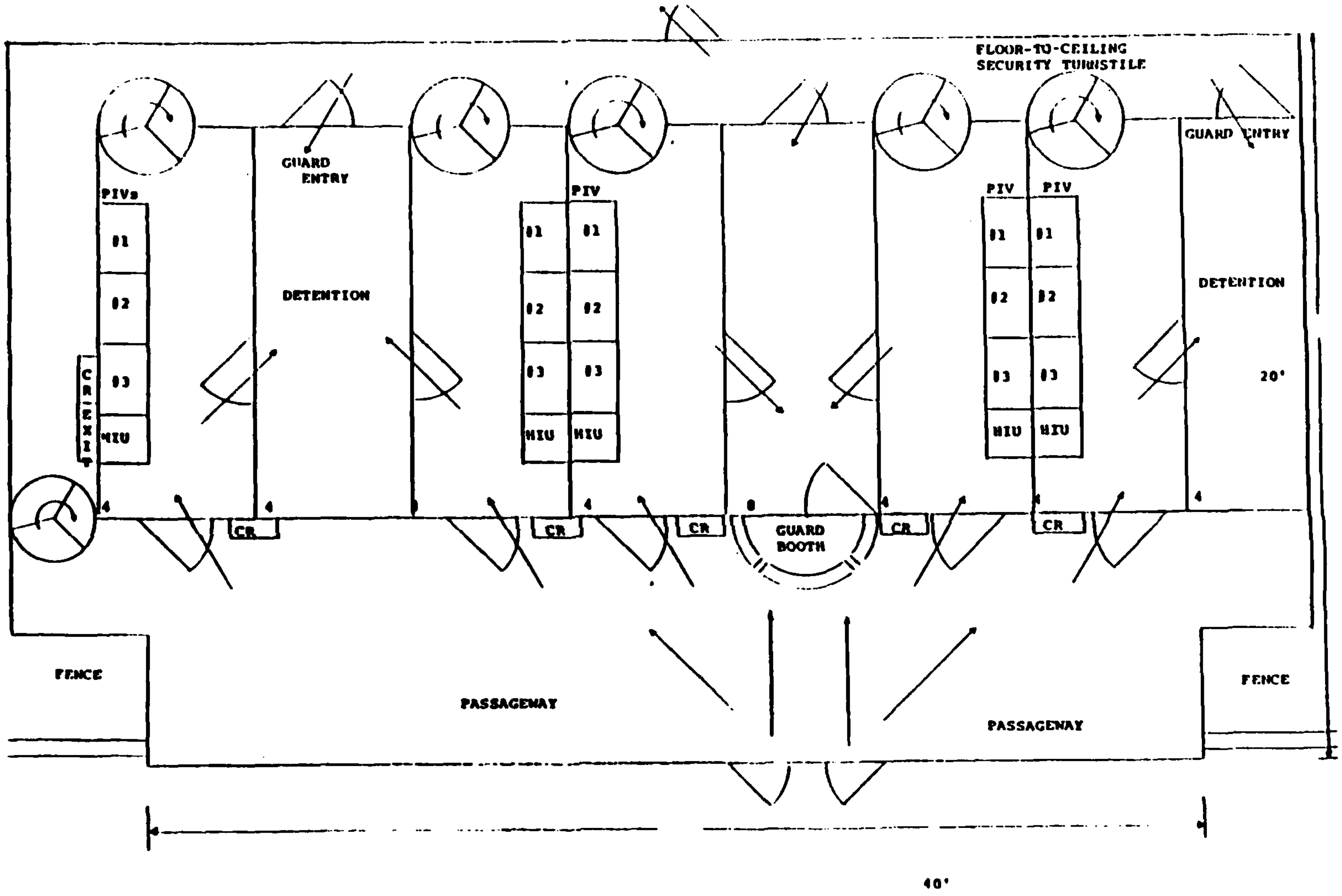


Figure 8-1: MODEL OF A FIVE PORTAL ENTRY CONTROL POINT

4. attention to behavior betrayals of potential impostors near the portals

5. responses to Type I events at his accompanying portals

6. determination of portal equipment faults

7. monitoring portal maintenance activity

8. determination of portal shut down and/or reprioritization

9. Interface with the Central Security Office

10. Response to assaults against the portal as an element of the Perimeter.

Whether a keypad is used to enter the portal, or a card reader, a normal base-badge is typically a requirement for access and must be visible at all times on the person attempting entry while in the vicinity of the portal area. Visitors and temporary users may require special attention from the guard, special log-ins, communications with central, and other interfaces, much the same as is currently done by the guard, including rerouting to Enrollment or to a special Visitors Entry Point.

Prior to an entry attempt, any person approaching the area may exhibit behavior susceptible to interpretation and categorization by the guard. It would seem likely that such behavior could be constrained to a scenario, in which case guards could be trained to recognize any impending surreptitious assault on the technical equipment in the portal. Groundrules for such recognition would also include the procedure of routing all

parcels through the guards booth, in order to keep an impostor's electronic aids out of the portals.

Responses to a Type I/Type II event, of course, takes priority among the guard's overall activities. Events can exceed the low rate predicted for the system, wherever a significant portion of the population is undergoing a learning period in the operating procedures of the portal. For given base turnover statistics, any portal may expect at any time to have an unduly large share of "novices" attempting entry. The duty of the guard under these circumstances is to assist the authorized entrant to successfully interface with the Hybrid System and gain entry through the portal. The guard must expect to communicate with Security Central in those situations and obtain directions and judgments from those security personnal who have access to deterministic data influencing the response to the Type I event, especially in those cases when the determination is made that the entrant is not authorized to proceed further, and more stringent measures are required at the portal.

The portal guard also must act as the first level assessor of equipment-level malfunctions at the portal. Although the portal electronics contain their own diagnostics, confirmation of a fault in any equipment would principally be done by a guard, who may clear the fault, or may pronounce the requirement for further maintenance. This interface action is considered vital to maintain a semblance of throughput in the presence of sabotage attempts or in an unfavorable environment. It therefore becomes neccessary to specify the equipment/guard interface requirements to the designer in such ways as to lessen the skill level required of the guard performing this task. A typical malfunction in this category may include a stuck door latch, an intermittent card reader/keypad, a display failure, and the like.

In conjunction with Security Central personnel, the portal guard must determine the required actions in the event of portal shutdown, whether to reprioritize specific configurations internal to the portal and continue, or to void the portal altogether and schedule maintenance action on it.

An override is akin to a portal shutdown, in that Security Central has collected data during the entrant attempt, that warrants a manual intervention into the portal activity. For this, the portal guard can be considered an extension of Security Central in order to augment the override action. Appropriate communications in accordance with preordained procedures understood by the portal guard would be a necessary adjunct to the override. A conceivable override situation might occur if the score margin was not sufficient to overcome Security Central's judgment as to any wrong pointers in the Identity Profile. Normally, however, such override situations would not be expected to occur.

While a portal guard would not be expected to single-handedly repulse a physical assault on his Entry Control Point (Perimeter Security personnel would have responsibility for large scale assaults against any point of the Perimeter) he would be expected to see the shape of events leading to an assault, and to take counteraction. To this end, Entry Control and Physical/Perimeter Security become merged. Otherwise, they are considered separable subsystems reporting to Security Central and the Base Commander.

C. AT SECURITY CENTRAL

Guard personnel at the nerve center of the Entry Control System perform the following functions:

1. Establish control of system performance at all levels. This includes overseeing all systems operation and taking actions as required to maintain the desired level of performance. Act for the Base Commander.

2. Monitor current activity as described in system reports issued in accordance with scenarios indicated in Appendix A.

3. Determine action to be taken when events occur that threaten system performance, such as increased Type I rejection of users, excessive queueing, impostor manipulations, equipment malfunction, general assault, all in accordance with pre-ordained scenarios, and in conjunction with Physical Security personnel, as required.

4. Establish enrollment standards and review enrollment data for compliance; confirm that technical quality levels for Reference File Packages are being met.

5. Identify cut-off points on the goat list, and approve remedial action necessary to reduce the level of goats in the system.

6. Monitor raw data processing and confirm that proper confidence levels are being maintained through proper amounts and quality of raw data ingested.

7. Handle alarms on a case-by-case basis in accordance with scenarios, and impose the necessary

scrutiny of the Hybrid machine rejects in order to make a proper final decision on identity.

8. Monitor the reports showing malfunction status at portals and in Security Central; schedule and supervise all maintenance actions in the System.

9. Schedule all guard personnel and confirm that all personnel have undergone proper levels of training in the ECS.

10. Supervise Entry Control activities for any Special Events of the day.

D. AT ENROLLMENT

Mostly clerical activity is required of guard personnel at enrollment. To a large extent the overall procedural functions are not altered from the present enrollment process. These include:

1. extracting the necessary and sufficient set of personal features required for proper action of the PIV's.

2. obtaining pertinent personnel history data, including security data.

3. overseeing the proper tutelage by the user.

The Hybrid System, however, requires increased attention to the enrollment function in that it becomes the weakest link in the identity chain that an impostor could exploit. This places special importance on the following functions:

1. Diligence in checking identities and clearances against error or fraud.

2. Establish and follow a proper procedure for badge disbursement, especially lost or stolen badges.

3. Timely preparation of lockout lists.

4. Confirmation at the earliest time of the users proficiency rating on each PIV.

5. Assist each candidate as a possible goat and initiate appropriate followup activity.

APPENDIX A

SYSTEM REPORTS AND MANAGEMENT CONTROLS

Reports generated by the hybrid system are divided into four groups. Each group deals with information and measurements at the point in time when the measured phenomena becomes meaningful to a management control feedback loop. These time intervals give rise to immediate reports, reports that are generated daily, periodically generated reports, and those reports that are created only on demand. The combination of these four groups will provide for the confident operation of the system, the capability to fine tune the system to particular needs of individual facilities, and the capability to forecast system requirements.

The criteria used to define the reports are those principals that are standard to management control. The reports have been designed to be economical, where only the minimum information needed to control an event is included while providing a reliable picture of system operation. The reports contain the measured events that will themselves be significant or symptomatic of potentially significant developments. The reports are timely. If an event cannot be controlled by real time awareness, it will not be reported in real time. The reports are simple, so not to confuse and misdirect from what is to be controlled. Finally, the reports are operationally suitable with the focus on action and the measurements in a form suitable for the action-taker and tailored to his needs.

The processor responsible for the printing of the majority of reporting tasks is the C3P, where there is an

interface with intrusion detection report printing. In particular, data representing a threat to security will be handled through the EP processor for immediate attention by base security personnel. The presence of communication links between the C3P and EP permits many of the reports to be shipped from the Enrollment Processor after compilation and generation. Certain reports contain information so sensitive that a printed copy may represent a security threat. In that case, only a select few terminals will be allowed to display the data, and the C3P may be constrained to print the information.

A. REAL TIME REPORTS

Real Time Reports are created only for those events which can be controlled by a real time awareness. Such events are alarms, personnel control, system performance, device diagnostics, and individual transactions. With the exception of the transaction report, real time reports are designed to be displayed on the screen in front of the ECS operator. The transaction report will be printed as a line of data upon conclusion of each transaction. Each screen-full may also be printed or stored if so desired. The real-time control screens dealing with personnel and system performance will be alternately displayed at all times on the ECS operator's screen. Each screen will appear for typically, ten seconds, then the next screen will automatically appear. This display is under the control of the operator who may, through the use of assigned function keys, perform such functions as screen update, next screen, access schedules, access visitor files, and generate specific reports. A reference guide to function key assignment will be available at the control screen. The use of function keys in the command terminal allows virtually any report or function to be accessed by pressing only one key. The entire system has been designed

with simplicity in mind allowing operating personnel to perform their jobs with a minimum of training.

1. PERFORMANCE AND SYSTEM STATUS SCREEN

A screen which is always displayed as a primary indicator is the Performance and System Status Screen, Figure A-1. This screen displays information pertaining to the performance of the hybrid system. Additional data concerning device diagnostics, alarms, and planned maintenance is also displayed. This screen file is updated every two minutes or by charge, or upon operator demand. The performance section of the screen allows a continuous monitoring of how the system is performing. Displayed are the current OOD, the OOD start time, quantity of users during this OOD, both commanded error rates, the actual Type I error rate with confidence level and precision, total quantity of users since 12:01 AM, total quantity of rejections during the same period, the quantity of operational portals, and the average throughput time for all portals. The data to support this section of the screen is contained in the transaction record, the OOD file, and a file that contains tables from which the confidence and precision are calculated.

The section of the screen labeled "Entry Control System Device Diagnostics" provides a visual verification that all components of the hybrid system are functioning correctly. Each individual element in the hierarchy is checked periodically, returning a code indicating that the device is OK or an error has been discovered. As long as the response code indicates an OK condition, the section labeled status will show OK. In the event of an error and depending upon the severity of the error, the screen will either be interrupted by the alarm screen, or show a numbered fault at the responsible component. Further information showing the error type, location, device ID, operator response,

ENTRY CONTROL SYSTEM PERFORMANCE FOR (date) LAST UPDATE (time)

CURRENT OOD ____ OOD START TIME ____ USERS THIS OOD ____

COM TYPE 2 ____ COM TYPE 1 ____ ACT TYPE 1 ____ CONF ____ PREC ____

TOTAL USERS SINCE 12:01 ____ TOTAL REJECTIONS SINCE 12:01 ____

OPERATIONAL PORTALS ____ AVERAGE THROUGHPUT ____ SECONDS

ENTRY CONTROL SYSTEM DEVICE DIAGNOSTICS

SYSTEM	STATUS	ERRCODE	LOCATION	DEV ID	RESPONSE	TIME ERR
C3P	------	------	------	------	------	------
EP	------	------	------	------	------	------
IDENT	------	------	------	------	------	------
ICP	------	------	------	------	------	------
HIU	------	------	------	------	------	------
PIV	------	------	------	------	------	------
PHY SEC	------	------	------	------	------	------

PLANNED ALARMS ______ ACTUAL ALARMS ______ SINCE 12:01

PLANNED MAINTENANCE JOBS ______

Figure A-1: PERFORMANCE AND SYSTEM STATUS SCREEN

and time of occurrence will be displayed on another line when an error is found. Upon the identification of an error or failure, an audible signal will be generated attracting the attention of the operator. For most serious failures, a different screen will appear, operator-nullable along with the audible signal directing the operator through the proper procedures for dealing with the event.

A listing of the quantity of planned alarms is displayed along with the number of actual alarm occurrences for the day. The number of planned alarms comes from the alarm schedule file, while the number of actuals is determined from records in the alarm history file. Planned maintenance jobs reflects the contents from the maintenance schedule file applicable to today's date.

This screen, as well as all other screen displays, may be stored or printed out upon command. Upon update, the screen image is built using a temporary working file which is dumped to the screen at update completion. Temporary and working files are invisible to the user and are not automatically saved. Access to other reports and screens is available through the use of the function keys, the more important of which are listed at the bottom of each screen.

2. PERSONNEL CONTROL SCREEN

The Personnel Control Screen, Figure A-2, is another of the two screens which appear on the control terminal at all times. It provides information regarding the whereabouts of key base personnel as well as data on guards and visitors. A listing of the total number of personnel on the facility as well as the total number of temporary badges issued appears, and the entire screen is updated every thirty minutes or upon operator

__________ AFB ENTRY CONTROL SYSTEM PERSONNEL FOR (date)

		ON BASE (Y/N)
BASE COMMANDER	___________________________	____
CHIEF OF STAFF	___________________________	____
SECURITY CHIEF	___________________________	____
ECS OPERATOR	___________________________	____

TOTAL PERSONNEL ON BASE _____ AS OF (time) TEMPORARY BADGES ___

SECURITY PERSONNEL BY ASSIGNMENT			VISITORS BY TYPE		
ASSIGNMENT	PLANNED	ON BASE	TYPE	PLANNED	ON BASE
ECS CONTROL	_______	_______	V.I.P.	_______	_______
PERIMETER TOUR	_______	_______	CONTRACTOR	_______	_______
FIRE WATCH	_______	_______	PRESS	_______	_______
ALARM RESPONSE	_______	_______	PART TIME	_______	_______
ESCORT	_______	_______	TECHNICAL	_______	_______
SPECIAL ASSMT.	_______	_______	EXT. FACILITY	_______	_______
ADMIN/MANAG	_______	_______	OTHER	_______	_______
OTHER	_______	_______			
TOTAL	_______	_______	TOTAL	_______	_______

Figure A-2: PERSONNEL CONTROL SCREEN

demand. The lower half of the screen is used to display security personnel by assignment, and visitors by type scheduled for the current day. Automatic determination of who is on base is accomplished by checking the transaction record for special guard and visitor ID numbers and incrementing the associated totals in each category. At the same time, each update causes the software to search the records to determine who has exited the facility, automatically decreasing the on-base totals. Through this screen, the operator has access to all information concerning personnel. The bottom of the screen lists function key assignments allowing the operator to selectively examine any schedule, personnel file, temporary badge file, or other screen.

The personnel control screen is supported primarily by the transaction record which is used to determine who is on base. The schedules files are used once each day by this screen to determine the planned number of guards per assignment and the number of scheduled visitors by type for the day. Upon each update, either timed or requested, a temporary file is created containing an image of the screen. When all of the checking and totaling is accomplished, the image is routed to the screen and displayed along with the time of update completion in the AS OF location.

3. PERFORMANCE BY PORTAL SCREEN

One of the screens available to Base Security personnel through the Performance Screen is the Performance by Portal Screen, Figure A-3. This screen displays information for each portal and is a more detailed examination of system performance. This is a two page screen which is scrolled upon request by the operator. All information used in this display comes from the transaction record with the exception of the commanded error rate, which comes from the ODD file. This screen

```
TYPE I ERROR PERFORMANCE BY PORTAL FOR (date) : (time)

PORTAL ID  # USER  # REJ  TIERR  CONF  COMERR  AVG TPUT  ALARMS
---------  ------  -----  -----  ----  ------  --------  ------
xx         xxxx    xxx    x.xxx  xx    x.xxx   xxx secs  xx






(INFORMATION IS LISTED FOR ALL PORTALS.  SCROLLING AT REQUEST)
```

HEADING	DEFINITION
PORTAL ID	The identification of the portal.
# USER	The quantity of individuals using the specified portal.
# REJ	The quantity of individuals rejected at the portal.
TIERR	The Type I error rate for the specified portal.
CONF	The confidence in the Type I error rate.
COMERR	The Type I error rate the system is commanded to operate at.
AVG TPUT	The average throughput time for the portal.
ALARMS	The quantity of alarms occuring at the portal.

Figure A-3: PERFORMANCE BY PORTAL SCREEN

is useful in spotting hardware degradation, throughput problems, and traffic patterns. Information included on this screen consists of the portal ID, the total quantity of users processed since 12:01 AM, the total quantity of rejections since 12:01 AM, the Type I error rate with associated confidence level, the commanded Type I error rate, the average throughput for the portal, and the number of actual alarms occurring since 12:01 AM. This screen may be requested at any time and covers all information in the transaction record up to the most recent entry attempt.

4. ALARM SCREEN

The Alarm Screen, Figure A-4, is generated upon each ECS alarm occurrence. Upon the discovery of an alarm, an audible signal is generated, despite what is currently on the screen, and an interrupt is produced causing the alarm handling software to take over. The alarm screen is displayed along with a custom designed map of the affected area which pinpoints the exact location of the alarm. The map lists the map number and the location in text of the affected areas. The screen automatically lists the alarm condition, the date and time, priority, planned response in code and text, and the planned response personnel. The operator must input his response to the event, and the event conclusion code. An area of the screen form has been allowed for responses other than planned in the space labeled Extenuating Circumstance Response. Upon event conclusion, the time is recorded as well as a code indicating the existence of multiple alarm occurrences.

The information used by this screen comes from the alarm file which contains the maps and English text for each alarm condition, along with planned responses and personnel. A historical record of each alarm is kept in the Alarm History

ALARM CONDITION ____________________

DATE _____ TIME _____ PRIORITY _____

PLANNED RESPONSE __________________

RESPONSE PERSONNEL ________________

RESPONSE __________________________

EXTENUATING CIRCUMSTANCE RESPONSE

____

____

EVENT CONCLUSION CODE _____________

TIME OF EVENT CONCLUSION __________

MULTIPLE ALARMS ? _________________

ALARM TEXT

____

____

____

____

____

MAP # ___ AREA ________

(GRAPHICS MAP)

Figure A-4: ALARM INFORMATION SCREEN

File after disposition. This file is updated at each alarm occurrence using the real time alarm screen as input. The screen remains active until the event conclusion code is entered. In the event of multiple alarms, the higher priority alarm condition will be displayed on the screen and an image of the current screen is saved until it can be dealt with. The operator has the option of saving any alarm screen temporarily and displaying any other screen. To preclude faulty handling by the operator, the system performance and status screen will show a fault until the operator has properly dealt with the event.

5. TRANSACTION REPORT

An historical record is maintained for every transaction that occurs in the hybrid system. This record is vital. It allows for a detailed examination of each user and how the user interacts with the system. It also shows the movements of all personnel on and off the facility allowing base management personnel to trace any previous entry activity. Transaction records are kept in two fashions. The first is a printed record detailing each entry attempt and printed upon the conclusion of the transaction. The second manner is a random access disk record. The disk file is the primary support for many of the management reports and contains more detailed information than the printed report.

The Transaction Report, Figure A-5, is printed continuously as long as there are transactions to report. It consists of data listing the user's ID in hex code, the time of the transaction, where the entry attempt occurred, the OOD in effect, the match scores and thresholds used by each PIV device, the throughput time, any alarms occurring at the time, and the final accept/reject decision of the HIU. The Transaction Report is not displayed on the screen but any part of the record can be

DATE ---------

USER	TIME	OOD	PORT	1TD	1MS	2TD	2MS	3TD	3MS	ALM	TPUT	SYS A/R
xxxx	xxxx	xx	xx	xx	xx	xx	xx	xx	xx	xxx	xx.x	x

HEADING	DEFINITION
USER	The ID of the user in hex.
TIME	The time of the card insertion.
OOD	The OOD in effect during this transaction.
PORT	The portal ID.
iTD	The threshold used by device i.
iMS	The match score from device i.
ALM	The coded ID of any alarm occuring at the portal during this entry attempt.
TPUT	The elapsed time from card insertion to portal exit.
SYS A/R	The final accept/reject decision from the HIU.

Figure A-5: PRINTED TRANSACTION REPORT

selectively examined using the Transaction Trace Report.

B. DAILY REPORTS

While real time reports have been designed for use by Base Security operating personnel, daily reports are intended for the use of base management. These reports are usually generated during the first lull in entry activity, around 10:00 AM. Most of the data used in the daily reports is collected during the morning rush of entry activity and represent system operation during the prior period.

1. SYSTEM SUMMARY

The first report to be automatically generated during the lull is the System Summary, Figure A-6. This is essentially an overview of performance and scheduling. It is designed to provide, at a glance, how well the system has performed, the expected alarms, the number of visitors expected daily, planned and non-planned maintenance, manpower requirements, and the quantity of password violations that have occurred since last report. This report may be displayed on a screen or, if a hard copy is desired, it may be printed out. The information contained in this report is gathered from the transaction record as well as other histories and from various schedules keyed in earlier.

2. GOAT STATISTICS BY PORTAL

A means of dealing with Type I goats on a more timely basis than that provided by the batch processing goat lists is included in the report entitled "Goat Statistics By Portal", Figure A-7. This listing provides goat data broken

```
SYSTEM SUMMARY FOR (date) ,CURRENT TIME _____
SYSTEM PERFORMANCE SINCE 12:01 AM
OOD #USERS #REJ COMERR ACTERR CONF PREC TPUT COMT2ERR OPPORT
xx  xxxxxx xxx   x.xx   x.xx   xx   .xx  xxx   x.xx     xx

ALARMS SINCE 12:01 AM    PLANNED _____    ACTUAL _____

VISITORS    TOTAL PLANNED _____  TOTAL VISITORS ON BASE _____
PLANNED VISITORS BY TYPE
VIP  PRESS  PART TIME  TECH  EXT FAC  OTHER  CONTRACTORS
xxx   xxx      xxx      xxx    xxx     xxx       xxx

MAINTENANCE   SCHEDULED JOBS _____   NO-SCHEDULED JOBS _____
TOTAL SYSTEM DOWN-TIME  _____    AS PERCENT UP-TIME   _____ %

MANPOWER    TOTAL HRS FOR SYSTEM OPERATION  _____ HRS
MANPOWER BREAKDOWN
ECS CONTROL     GUARDS     ADMINISTRATIVE   MAINTENANCE   OTHER
    xxx          xxx            xxx              xxx        xxx

PASSWORD VIOLATIONS SINCE 12:01 AM  _____
```

HEADING	DEFINITION
OOD	The OOD in effect.
#USERS	The quantity of users.
#REJ	The quantity of rejections.
COMERR	The commanded Type I error rate.
ACTERR	The actual error rate.
CONF	The confidence in ACTERR.
PREC	The precision in ACTERR.
TPUT	The average throughput.
COMT2ERR	The commanded Type II error rate.
OPPORT	The quantity of operational ports.

Figure A-6: SYSTEM SUMMARY OPERATIONS REPORT

```
GOAT STATISTICS BY PORTAL FOR (date)
PORTAL  OOD  MISSES BY   TOTAL  TOT PORT  TOT T1  POSS NEW
             PIV DEV            REJECTS   GOATS   GOATS
  xx     xx  xx xx xx     xxx     xx        xx      xx









     (ALL PORTALS WILL BE LISTED)
```

HEADING	DEFINITION
PORTAL	The ID of the portal.
OOD	The OOD in effect.
MISSES BY PIV DEV	The quantity of non-matches for each PIV.
TOTAL	The total quantity of misses for all PIVs in the specified portal.
TOT PORT REJECTS	The quantity of users rejected.
TOT T1 GOATS	The quantity of Type I goats processed by the portal for this time period.
POSS NEW GOATS	The quantity of possible new goats discovered within this time frame.

Figure A-7: GOAT STATISTICS BY PORTAL REPORT

down by portal. Included data consists of the OOD, the quantity of misses (non matches) for each PIV device, the total quantity of HIU rejections, the total quantity of Type I goats processed, and the quantity of possible new goats discovered during the reporting period. Identification of goats is a highlighted feature of the hybrid system and a means of early identification results in corrective measures being undertaken before the goat becomes "chronic." The report generating software identifies possible goats by using the same technique defined under the Performance Control Algorithm. If a user not previously identified as a goat is rejected, the category labeled "Possible New Goats" is incremented and the user's name is stored in a daily possible goat file. The contents of this file may be displayed on terminals having the proper security clearance. Upon identification, the possible new goat may be called upon to re-enroll, be re-instructed, or simply be kept under observation.

3. THROUGHPUT BY PORTAL

A factor vital to the performance of the hybrid system is the amount of time each user spends gaining entrance to the facility. A detailed examination of this throughput is provided by the report entitled "Throughput by Portal," Figure A-8. The report is a breakout of the average time taken to proceed through the portal. Included in the report are the portal ID, the quantity of users passing through the portal, the average throughput time, the average time each user takes to address the first PIV device, the average time from PIN entry to system A/R, the time from system A/R to exit, the lengthiest throughput time, the shortest throughput time, the quantity of rejections during the report period, the quantity of alarms occurring at the portal,and the number of operating PIVs within the portal. All of the data used to compile this report is obtained from the transaction record. Daily comparisons of throughput rates are

```
THROUGHPUT BY PORTAL FOR (date) ,CURRENT TIME _______
PORT USERS TPUT ADD PRC EXIT BEST WORST #REJ ALMS OP PIV
xx   xxxx  xx   x.x x.x x.x  x.x  x.x    xx   xx    xx
```

(ALL PORTALS WILL BE LISTED)

HEADING	DEFINITION
PORT	The portal ID.
USERS	The quantity of individuals attempting entry at the specified portal.
TPUT	The average throughput time.
ADD	The average time for each user to address the first PIV device.
PRC	The average time from PIN entry to system A/R.
EXIT	The average time from A/R to portal exit.
BEST	The best throughput time (door to door).
WORST	The lengthiest throughput time.
#REJ	The quantity of system rejections.
ALMS	The quantity of alarms.
OP PIV	The quantity of operational PIVs.

Figure A-8: THROUGHPUT BY PORTAL REPORT

possible by generating this report for the periods to be compared. While this report is automatically generated daily, the software will allow the report to be generated for any day.

4. ALARM PERFORMANCE REPORT

The ability to monitor the effectiveness of security personnel in their reponse to alarm conditions is included in the report labeled "Alarm Performance Report", Figure A-9. This daily-created report details alarm occurrences for the previous twenty-four hours using the records kept in the alarm history file. It contains data on all alarms both planned and actual. The time of alarm occurrence is listed along with the alarm condition, the affected area, the map number displayed with the alarm, the operator's response, any response resulting from extenuating circumstances, which includes actions from the responding guards, the duration of the event, and the disposition at event conclusion. Alarm conditions are broken down by threat for filing purposes. The three classifications of alarms are life threatening, security threatening, and data threatening. All classes will be included in the report.

5. PASSWORD VIOLATIONS

A report designed as an early warning for possible security violations is entitled "Password Violations," Figure A-10. This report, which is automatically generated at least once a day, covers all password violations occurring during the period. The included information consists of the time of violation occurrence, the ID of the operator who caused the violation, the terminal ID, and the unauthorized password or code. The violations are automatically recorded as they occur in the password violation history file.

ALARM PERFORMANCE FOR (date) ALARM CLASS _____ CURR TIME _____

TIME	ALARM	AREA	MAP#	RESPONSE	EXT CIRC	EV DUR	RESULT
xx:xx	xxxxxx	xxx	xxx	xxxxxxx	xxxxxxx	xx:xx	xxx

(ALL ALARMS OCCURING WITHIN THE TIME FRAME ARE LISTED)

HEADING	DEFINITION
TIME	The time of alarm occurance.
ALARM	The actual alarm condition.
AREA	The affected area.
MAP#	The map number displayed.
RESPONSE	The response input by the operator (coded).
EXT CIRC	Additional operator responses input as a result of extenuating circumstances.
EV DUR	The duration of the event.
RESULT	Disposition at event conclusion.

Figure A-9: ALARM PERFORMANCE REPORT

```
PASSWORD VIOLATIONS SINCE 12:01 AM FOR (date)
TIME       OPERATOR ID    TERMINAL ID    UNAUTHORIZED
                                         PASSWORD/CODE
xx:xx      xxxx           xx             xxxxxxx








(ALL VIOLATIONS WILL BE LISTED FOR THIS DATE)
```

Figure A-10: PASSWORD VIOLATIONS REPORT

6. TEMPORARY BADGE REPORT

For varying reasons, every user will not have his identification card in his possession. These cards, which are vital to the operation of the ECS, will undoubtedly be misplaced and/or forgotten. When this occurs, a temporary badge must be assigned to the user and his regular badge ID must be de-authorized. To keep track of the temporary badges used in the system, the report entitled "Temporary Badge Report," Figure A-11, will be generated at least once a day. This report is created from data input by the person issuing the temporary badge, which is kept in a history file. Included information consists of the time of card issuance, the name and ID of the user assigned the card, the temporary ID number of the badge, the reason for the issuance of the card, and the time frame during which the card may be used. Whenever a temporary badge is issued, the user's regular badge will no longer admit him to the facility. In order to reauthorize the regular card, the user must return the temporary badge, have it deauthorized, and have a new regular badge instated. This reauthorization activity is documented in a report generated at least weekly entitled "Authorization History."

7. SCHEDULES

All schedules are available to the operating personnel through the primary screens. By pushing one function key, an operator may display the schedules menu, Figure A-12. This menu lists schedules for guards, visitors, maintenance, alarms, enrollment, special events, and a catch-all "other" schedule. Each schedule on the main menu is further broken down into sub-files containing the detailed information on all scheduled activity. By pushing the menu keys, the operator may proceed through each menu until he arrives at the information of

```
TEMPORARY BADGE REPORT FOR (date) : TOTAL TEMP BADGES ISSUED _____
TIME    ID    NAME                  TID#   REASON              AUT TF
xx:xx  xxxx  xxxxxxx                xxxx    xxxxxxx            xxxx:xxxx
```

(ALL USERS REQUIRING TEMPORARY BADGES FOR THIS DATE WILL BE LISTED)

HEADING	DEFINITION
TIME	The time of badge issuance.
ID	The user's original ID.
NAME	The user's name.
TID#	The ID of the badge issued.
REASON	The reason for badge issuance.
AUT TF	The authorized time frame during which the badge may be used.

Figure A-11: TEMPORARY BADGE REPORT

```
                    SCHEDULES MENU

                 1.   GUARDS
                 2.   VISITORS
                 3.   MAINTENANCE
                 4.   ALARMS
                 5.   ENROLLMENT
                 6.   SPECIAL
                 7.   OTHER
                 8.   ESCAPE


      PRESS THE NUMBER OF THE REQUIRED SCHEDULE,
      NUMBER 8 RETURNS TO CONTROL SCREENS  ---
```

```
                    GUARD SCHEDULES MENU

                 1.   ENTRY CONTROL PERSONNEL
                 2.   PERIMETER TOUR
                 3.   FIRE WATCH
                 4.   ESCORT
                 5.   SPECIAL ASSIGNMENT
                 6.   ALARM RESPONSE
                 7.   ADMINISTRATIVE-MANAGEMENT
                 8.   OTHER
                 9.   ESCAPE


    PRESS THE NUMBER OF THE REQUIRED GUARD SCHEDULE,
    NUMBER 9 RETURNS TO MAIN SCHEDULE MENU  ---
```

Figure A-12 (1 OF 3): SCHEDULES MAIN MENU AND GUARD SCHEDULE SUB-MENU

```
                VISITORS SCHEDULE MENU

                1.  VIP
                2.  CONTRACTOR PERSONNEL
                3.  PART-TIME PERSONNEL
                4.  TECHNICAL
                5.  EXTERNAL FACILITY
                6.  PRESS
                7.  OTHER
                8.  ESCAPE

PRESS THE NUMBER OF THE REQUIRED VISTOR SCHEDULE,
NUMBER 8 REURNS TO MAIN SCHEDULE MENU  ---
```

```
              MAINTENANCE SCHEDULE MENU

    HARDWARE                        SOFTWARE

    1.  UPGRADE                     6.  UPGRADE
    2.  REPAIR                      7.  CORRECT-DEBUG
    3.  CLEANING                    8.  TEST
    4.  TEST                        9.  OTHER
    5.  OTHER                       0.  ESCAPE

PRESS THE NUMBER FOR THE REQUIRED MAINTENANCE SCHEDULE,
NUMBER 0 RETURNS TO MAIN SCHEDULE MENU  ---
```

Figure A-12 (2 OF 3): VISITOR AND MAINTENANCE SCHEDULE SUB-MENU

```
                    ALARMS SCHEDULE MENU

                    1.  LIFE THREATENING ALARMS
                    2.  SECURITY THREATINING ALARMS
                    3.  DATA/EQUIPMENT THREATENING ALARMS
                    4.  OTHER
                    5.  ESCAPE

          PRESS THE NUMBER OF THE REQUIRED ALARM SCHEDULE,
          NUMBER 5 RETURNS TO THE MAIN SCHEDULE MENU  ---
```

```
                    ENROLLMENT SCHEDULES MENU

                    1.  NEW ENROLLMENTS
                    2.  RE-ENROLLMENTS
                    3.  DE-ENROLLMENTS
                    4.  ESCAPE

       PRESS THE NUMBER OF THE REQUIRED ENROLLMENT SCHEDULE,
       NUMBER 4 RETURNS TO THE MAIN SCHEDULE MENU  ---
```

Figure A-12 (3 OF 3): ALARM TEST AND ENROLLMENT SCHEDULE SUB-MENU

interest. Scheduling is an important aspect of the hybrid system allowing optimum personnel deployment, resource control and a means of controlling visitors and maintenance.

8. GUARD SCHEDULES

Guard schedules, Figure A-12, are broken down into eight separate categories. These are entry control personnel, perimeter tour, fire watch, escort, special assignment, alarm response, administrative-management, and other. These assignments must be pre-planned and input to the proper file in advance by clerical personnel. This can be accomplished daily, weekly, or monthly. The information available through the schedule, Figure A-13, consists of the ID of the assigned guard, his name, the job code, the time frame for duty, the assigned area, and alternate guard in case of absence, the communication ID or phone number assigned to the guard, and the name of the officer who authorized the duty. The report lists those guards on duty for the day. These schedules for Entry Control are integrated with schedules for other Security Subsystems, i.e. Physical Security, etc.

9. VISITORS SCHEDULE

All visitors to the secure facility must be scheduled. For ease of reference, visitors have been placed into categories by type. These categories are VIP, contractors, part-time personnel, technical personnel, military visitors denoted as external facility, members of the press, and the catch-all "other" category. This list is displayed by the menu labeled "Visitors Schedules Menu," Figure A-12. The displayed schedule, Figure A-14, consists of the visitor's ID number, name, security level clearance, authorized time frame for the visit, name of the company or military base the visitor is affiliated with, ID of

```
                              GUARD SCHEDULES
ASSIGNMENT _______________ FOR  (date)
ID     NAME              JOB CODE   TIMES   AREA  ALT  COM  AUTH
xxxx   xxxxxxxxxxx         xxxx     xxxxxx  xxxx  xxxx xxx  xxxxxx









(ALL GUARDS ASSIGNED THIS DUTY WILL BE LISTED FOR THE DATE)






     HEADING          DESCRIPTION
     -------          -----------
     ID               The guard ID.
     NAME             The name of the assigned guard.
     JOB CODE         The specific job assigned.
     TIMES            The time frame for the assigned duty.
     AREA             The area assigned.
     ALT              The ID of an alternate.
     COM              The communications ID of the guard.
     AUTH             The authorizing officer.
```

Figure A-13: GUARD SCHEDULE SCREEN

```
                    VISITORS SCHEDULE FOR  (date)
VISITOR TYPE    (name of sub-file)
VID       NAME          SLC  AUT TF    AFFIL    ESCORT    TIME  TOSEE
xxxx      xxxxxxxxxx    xxx  xxxxxx    xxxxx    xxxxx     xxxx  xxxxxxx








(SCHEDULED VISITORS OF THE SPECIFIED TYPE WILL BE LISTED)






      HEADING            DESCRIPTION
      -------            -----------
      VID                The assigned ID of the visitor.
      NAME               The visitors name.
      SLC                The security level clearence of the visitor.
      AUT TF             The authorized time frame.
      AFFIL              The company/base of the visitor.
      ESCORT             The ID of the escort.
      TIME               The arrival time of the visitor.
      TOSEE              The person the visitor is to see.
```

Figure A-14: VISITORS SCHEDULE SCREEN

the designated escort, Portals to be accessed, expected time of arrival, and name of the person the visitor is to see. All of this information is input to the appropriate file by clerical personnel in advance of the visit. More detailed information is available on the visitor through the visitor report which will be described later.

10. MAINTENANCE SCHEDULE

Scheduled maintenance of the ECS is divided into two major groups depending on the type. The two groups are hardware and software maintenance. Each major group is further subdivided into the categories listed in Figure A-12, labeled "Maintenance Schedule Menu." The maintenance schedule contains data regarding the job number, the affected areas, the specific equipment or program to be worked on, the planned start time, the planned stop time, the IDs of the assigned technical people, and the name of the authorizing officer. This report, like all other schedules, draws from information input in advance. The report as it will appear on the screen is illustrated in Figure A-15.

11. ALARM SCHEDULE

The scheduling of alarm tests is divided into the three categories of threat. The alarm test schedules menu, Figure A-12, illustrates this breakout. The alarm test schedule itself is shown in Figure A-16. The included information is the actual alarm to be tested, the time it will be tested, the areas that will be affected, the planned response to the alarm, the planned duration of the alarm, the planned response personnel, and the name of the authorizing official. The alarm test schedule used in conjunction with the alarm performance report should provide a means to fine tune the responses in accordance with the dictates of security.

```
                  MAINTENANCE SCHEDULE FOR  (date)
MAINTENANCE TYPE  (sub-file name)
JOB#  AFFAREAS  AFF EQ/PROG   START  STOP  TECHID  AUTH
xxxx  xxxxxx    xxxxxxxxx     xxxxx  xxxxx xxxxx   xxxxxxxx









(ALL JOBS SCHEDULED FOR THIS DATE AND TYPE WILL BE LISTED)





     HEADING          DESCRIPTION
     -------          -----------
     JOB#             The number assigned for the task.
     AFFAREAS         The areas affected by the job.
     AFF EQ/PROG      The equipment or program to be worked on.
     START            The planned start time.
     STOP             The planned stop time.
     TECHID           The ID(s) of the assigned personnel.
     AUTH             The name of the authorizing officer.
```

Figure A-15: MAINTENENCE SCHEDULE SCREEN

ALARM SCHEDULE FOR (date)

ALARM CLASSIFICATION (sub-file name)

ALARM	TIME	AREA	RESP	DUR	RESP PERS	AUTH
xxxxx	xxxx	xx, xx	xx,xx	xxxx	xxxx	xxxxxxxx

(PLANNED ALARMS OF THE SPECIFIED CLASSIFICATION WILL BE DISPLAYED)

HEADING	DESCRIPTION
ALARM	The specific alarm to be tested.
TIME	The planned time of occurance.
AREA	The areas affected.
RESP	The planned response (coded).
DUR	The planned duration.
RESP PERS	The planned response personnel.
AUTH	The authorizing officer.

Figure A-16: ALARM TEST SCHEDULE SCREEN

12. ENROLLMENT SCHEDULES

Enrollment schedules are divided into categories dependent on the type of activity. The "Enrollment Schedules Menu," Figure A-12, details this breakdown showing the sub-schedules as new, re-, and de-enrollments. The enrollment schedule, shown in Figure A-17, lists the ID and name of the user, the planned time the user should report to the enrollment center, and the name of the person authorizing the activity.

13. SPECIAL EVENTS

The special events file is a catch-all for scheduled activity not covered by the previously defined schedules. Its format is simple in order to be universal. The special event is written to the file labeled "Special Events" with no specific format requirements other than the date. Upon request, the contents of this file will be displayed in the same format used when written. This report displays only the special events occurring on the date of the request, but, as with all other schedules, the software has the included capability to display any schedule for any date. This, however, requires an input in the form of the date to be viewed and involves more than pressing one function key. Minimal operator training is required to utilize these additional software features.

14. DAILY REPORT STORAGE

The daily reports are not all printed out immediately upon compilation. They are stored in a temporary daily report file which is updated and overwritten each time a new report is generated. In this fashion, the reports may be displayed on various screens throughout the day by whoever needs the information. If a permanent record of the report is required, a

```
ENROLLMENT SCHEDULES FOR  (date)
ACTIVITY TYPE   ( new, re, de )  ENROLLMENT
ID     NAME                 TIME       AUTH
xxxx  xxxxxxxxxx            xxxxxx     xxxxxxxxxx









(SCHEDULED ENROLLMENTS - THIS DATE AND TYPE WILL BE DISPLAYED)






     HEADING          DESCRIPTION
     -------          -----------
     ID               The ID of the enrollee.
     NAME             The name of the enrollee.
     TIME             The time enrollee is to report.
     AUTH             The authorizing officer.
```

Figure A-17: ENROLLMENT SCHEDULE SCREEN

printed copy may be produced at any time providing the proper authorization parameters are met. Schedules are kept in storage for only a short time to conserve space. The visitors schedule is an exception. This schedule has complete information on all visitors and is essentially a history of visitor activity. For this reason the visitors schedules are kept on large disks along with the other histories. The visitors schedule turned history is used by the visitors report software to generate future reports.

C. PERIODICALLY GENERATED REPORTS

Periodically generated reports are those reports created weekly, as in the case of the histories, or bi-monthly, such as the reports resulting from batch processing error data. The batch processed error data provides vital information regarding the ability of the system to provide security, a means of comparing individual device technologies, and an idea of how the population of the facility interacts with the hybrid system. All periodic reports are designed to be displayed on a CRT, but hard copy may be generated as desired.

1. WEEKLY HISTORY SUMMARY REPORT

The history summary provides information for all history files except the OOD history and visitors history which is available in other displays. It consists of a summary of alarms for the week, the quantity of programming/file changes, the quantity of authorization changes, enrollment activity, maintenance activity, and a listing of the operational hours since system initialization. This report is a quick overview of system activity, with the bulk of the relevant data contained in the various history reports themselves. The report format is shown in Figure A-18.

SYSTEM HISTORY SUMMARY FOR WEEK ENDING (date)

ALARMS: TOTAL PLANED _____ TOTAL ACTUAL _____ AVG TIME CONCL _____

LIFE THREAT	_____	_____	_____
SECURITY THREAT	_____	_____	_____
DATA THREAT	_____	_____	_____

PROGRAMMING/ FILE CHANGES TOTAL PROG/FILE CHANGES _____

UPGRADE _____ TEST _____ DEBUG _____ NEW _____

AUTHORIZATION CHANGES TOTAL CHANGES _____

TOTAL DE-AUT _____ TOTAL RE-AUT _____ TOTAL NEW-AUT _____

ENROLLMENT ACTIVITY TOTAL ENROLLMENTS _____

TOTAL NEW _____ TOTAL RE- _____ TOTAL DE- _____

MAINTENANCE ACTIVITY TOTAL SCHED'D _____ TOTAL NON-SCHD'D _____

UPGRADE _____ REPAIR _____ TEST _____ CLEAN _____ OTHER _____

HOURS SINCE SYSTEM INITIALIZATION ______ OPERATIONAL HOURS _____

SYSTEM DOWNTIME AS A PERCENT OF TOTAL HOURS ______ %

Figure A-18: WEEKLY HISTORY SUMMARY REPORT

2. ALARM HISTORY REPORT

The alarm history report, like all other histories, is a chronological record of activity. The report is automatically generated for the previous week but may be specified to list alarms by condition or for a different time frame. Information included in the report, shown in Figure A-19, shows the date of occurrence, the time of occurrence, the alarm condition, the priority, the ID of the control operator, the IDs of the response personnel, the time of event conclusion, the map number, the affected areas, the operator's response translated from code, the extenuating circumstance response usually input by the response personnel, and the disposition upon event conclusion. All data is obtained from the alarm history file. Each alarm, planned and actual, occurring within the specified time frame will be listed.

3. PROGRAMMING HISTORY REPORT

Anytime the system's data base or programming is changed, a potential security threat exists. To provide a means of recording and monitoring changes, a report entitled "Programming History Report," Figure A-20, will be generated weekly. This report displays information consisting of the date of change, the time of change, the terminal the change was made through, the ID of the operator and his security level clearance, the reason for the change, the name of the authorizing officer, the name of the program, or file, the data change, and the data inserted. This report has an included capability of being specified for any time frame, allowing examination of any change occurring to the system. The history is chronological and automatic. The intent is to keep it from being overridden and to record all changes after system initialization.

```
ALARM HISTORY REPORT:  SPECIFIED FOR __________
DATE      TIME  ALARM    PR  OP ID  RESP ID  CONCL  MA  MAP  AREAS
xx/xx/xx  xxxx   xxx     xx   xxxx   xxxx     xxxx  x   xxx  xxxxx
OP RESP   ----------------------------------------------------------
EXT CIRC RSP  ------------------------------------------------------
DISP @ CONCL  -------------------




(ALARM HISTORY IS KEPT CHRONOLOGICALLY, AND MAY BE SPECIFIED BY
 DATE OR ALARM CONDITION.  ALL ALARMS OCCURING WITHIN THE
 SPECIFIED PARAMETERS WILL BE DISPLAYED AND/OR PRINTED)
```

HEADING	DESCRIPTION
DATE	The date of alarm occurence.
TIME	The time of alarm occurence.
ALARM	The specific alarm condition.
PR	The priority of the alarm.
OP ID	The ID of the C3P operator.
RESP ID	The ID of the response personnel.
CONCL	The time of event conclusion.
MA	Were there multiple alarm occurences ?
MAP	The map number displayed.
AREAS	The C3P operator's response.
EXT CIRC RSP	Responses resulting from extenuating circumstances.
DISP @ CONCL	The final disposition at event conclusion.

Figure A-19: ALARM HISTORY SCREEN

```
PROGRAMMING HISTORY REPORT FOR TIME FRAME  (date)  TO  (date)
DATE      TIME    TER  OP ID  SLC   REASON    AUTH
xx/xx/xx  xx:xx   xx   xxxx   xx    xxxxxxx   xxxxxxxxx
PROGRAM/FILE NAME  -------------------
OLD DATA  ---------------------------------------------------
NEW DATA  ---------------------------------------------------





(ALL PROGRAMMING CHANGES OCCURING WITHIN THE TIME FRAME ARE LISTED)
```

HEADING	DESCRIPTION
DATE	The date of activity.
TIME	The time of activity.
TER	The ID of the terminal used.
OP ID	The ID of the operator.
SLC	The security level clearance of the operator.
REASON	The reason for the change.
AUTH	The authorizing officer.

Figure A-20: PROGRAMMING HISTORY REPORT

4. AUTHORIZATION HISTORY REPORT

The authorization history report is included in the periodically generated reports because it is a history. It is expected, however, that this report will be generated on a daily basis and possibly twice daily. The report, illustrated in Figure A-21, contains the date of authorization change, the ID of the user, the user's name, the type of change, and the reason for the change. This report may be specified to list all authorization changes occurring over a given time frame if so desired.

5. ENROLLMENT HISTORY REPORT

Enrollment history, shown in Figure A-22, details enrollment activity for the previous week, or other specified time frame. It consists of the date of enrollment, the time, the ID and name of the user, the activity type, the ID of the enrollment center operator, and the name of the authorizing officer.

6. MAINTENANCE HISTORY REPORT

All maintenance activity is detailed by the report entitled "Maintenance History Report," Figure A-23. This report includes the date of maintenance, the time, the job number, the type of maintenance, the affected areas, the time of job conclusion, the ID numbers of the responsible maintenance personnel, the name of the authorizing official, the specific equipment worked on, the specific equipment replaced, the equipment or areas that were down as a result of the maintenance, and the final disposition. All maintenance, planned or non-planned, will be included in the report.

AUTHORIZATION HISTORY FOR TIME FRAME (date) TO (date)

DATE	ID	NAME	TYPE	REASON
xx/xx/xx	xxxx	xxxxxxxxx	xxxxxx	xxxxxxxx

(ALL AUTHORIZATION CHANGES OCCURING WITHIN THE TIME FRAME ARE LISTED)

HEADING	DESCRIPTION
DATE	The date of the change.
ID	The ID of the user.
NAME	The name of the user.
TYPE	The type of change
REASON	The reason for the change.

Figure A-21: AUTHORIZATION HISTORY REPORT

```
ENROLLMENT HISTORY REPORT FOR TIME FRAME  (date)  TO  (date)
DATE      TIME   ID   NAME         ACT TYPE  OP ID  AUTH
xx/xx/xx  xx:xx xxxx xxxxxxxxx      xxxx      xxxx  xxxxxxx








(ALL ENROLLMENT ACTIVITY FOR THE TIME FRAME WILL BE LISTED)
```

HEADING	DESCRIPTION
DATE	The date of the activity.
TIME	The time of the activity.
ID	The ID of the enrollee.
NAME	The name of the enrollee.
ACT TYPE	The type of activity (new, re-, de-).
OP ID	The ID of the operator.
AUTH	The authorizing officer.

Figure A-22: ENROLLMENT HISTORY REPORT

```
MAINTENANCE HISTORY FOR TIME FRAME  (date)  TO  (date)
DATE        TIME   JOB#  TYPE  AFFAREA  STOP  MAINTID   AUTH
xx/xx/xx  xxxx   xxx   xxx   xxxx     xxxx  xxxx      xxxxxx
EQUIPMENT:
REPLACED:
EQUIP/AREAS DOWN:
DISPOSITION:





(ALL MAINTENANCE OCCURING DURING THE TIME FRAME WILL BE LISTED)
```

HEADING	DESCRIPTION
DATE	The date of the maintenance.
TIME	The start time.
JOB#	The assigned job number.
TYPE	The type of maintenance.
AFFAREA	The areas affected.
STOP	The time of completion.
MAINTID	The ID(s) of the maintenance personnel.
AUTH	The name of the authorizing official.
EQUIPMENT	The specific items worked on.
REPLACED	Any equipment that was replaced.
EQUIP/AREAS DOWN	Any equipment that was down due to the activity.
DISPOSITION	The disposition at maintenance conclusion.

Figure A-23: MAINTENANCE HISTORY REPORT

7. OOD HISTORY REPORT

In order to gain a better understanding of the OODs and how they affect various factors in the system, a report detailing OOD changes is included. This report, shown in Figure A-24, lists the OOD, the date it was changed, the time it was changed, the date/time it was started, the commanded error rates, the actual Type I error rate with corresponding precision and confidence, and the average throughput during the OOD. Correlations may be drawn between the OOD, Type I error rate, and throughput which will be valuable for planning purposes. This report may be displayed only on authorized terminals and will be compiled by the C3P.

8. BI-MONTHLY REPORTS

Reports that are generated bi-monthly consist of information created as a result of batch processing error data. These reports provide information on Type I error, Type II error, and goats. This information is primarily used to reset the logical configuration tables. Score distribution curves, from which the error probability curves are generated, are included with this data to allow long-term examination of population trends. These reports also allow each PIV device to be compared against the other and evaluated for future device acquisition. Reports resulting from batch processing are kept in temporary storage until the next batch of reports becomes available. During this time they may be displayed on authorized screens. Hard copy will be generated for long-term storage and comparison purposes.

```
OOD HISTORY REPORT FOR WEEK ENDING  (date)
OOD  DATE      TIME  CHDATE    CHTIME  PREC   TPUT
xx   xx/xx/xx  xxxx  xx/xx/xx  xxxx    .xx    xxxx









(ALL OOD CHANGES OCCURING DURING THE WEEK WILL BE LISTED)
```

HEADING	DESCRIPTION
OOD	The OOD (coded).
DATE	The date the OOD started on.
TIME	The time the OOD started at.
CHDATE	The date the OOD was changed.
CHTIME	The time the OOD was changed.
PREC	The precision of the actual error rate.
TPUT	The average throughput for this OOD.

Figure A-24: OOD HISTORY REPORT

9. GOAT SUMMARY

The report labeled "Goat Summary," Figure A-25, is an overview of all goats within the base population. It lists actual and possible goats of both error types for all devices. Also included are the average scores for all users compared against the scores of actual goats of both error types.

10. GOAT REPORTS

Goat reports consist of a list of those users defined as goats during the batch processing period. The report format, Figure A-26, is the same for actual and possible goats of both error types for all devices. Included is the time frame covered by the BP period, the device type, the error type, the list type, the user's ID and name, his average score, the quantity of failures, and the total quantity of attempts or matches made by the user. In the case of Type II goats, the total attempts category will contain the total quantity of reference files the user's file was matched against. Goat data represents a security problem if the lists were to fall into the wrong hands. For that reason, it is not expected that the lists will be printed but rather displayed on authorized terminals only. This report on possible goats will prove to be useful in that the possible goats may be corrected or cured of their goat-like tendencies, precluding the security threat of becoming actual goats.

11. ERROR PERFORMANCE REPORTS

Error performance reports are generated for each device from match score distribution curves. Reports covering both error types with goats both included and excluded are available. Two formats are created depending on goat inclusion. The report labeled "True Performance Curve," Figure A-27, is a graphic

GOAT SUMMARY FOR TIME FRAME FROM (date) TO (date)

TOTAL USERS _____

DEVICE	T1PG	%POP	T1AG	%POP	T2PG	%POP	T2AG	%POP
ALL	xxx	xx.xx	xxx	xx.xx	xxx	xx.xx	xxx	xx.xx
#1								
#2								
#3								

DEVICE	AVG ALL USERS	AVG T1AG	AVG T2AG
#1	xx.xx	xx.xx	xx.xx
#2			
#3			

HEADING	DESCRIPTION
TOTAL USERS	The quantity of enrolled users.
DEVICE	The PIV device.
TnPG	The quantity of Type n possible goats.
TnAG	The quantity of Type n actual goats.
%POP	Percentage of the population.

Figure A-25: GOAT SUMMARY REPORT

GOAT REPORT FOR TIME FRAME (date) TO (date)

DEVICE TYPE __________

ERROR TYPE __________

LIST TYPE __________

USER ID	USER NAME	AVG SC	FAILURES	TOT ATT
xxxx	xxxxxxxxx	xx	xx	xxxx

(ALL USERS WITHIN THE SPECIFIED PARAMETERS WILL BE LISTED)

HEADING	DESCRIPTION
DEVICE TYPE	The type of device technology.
ERROR TYPE	Either Type I or Type II error.
LIST TYPE	Either actual or possible goats.
USER ID	Each user's ID.
USER NAME	Each user's name.
AVG SC	The average scre.
FAILURES	Quantity of failures.
TOT ATT	Total quantity of attempts.

Figure A-26: GOAT REPORT

display of error probability using data from all users in the hybrid system including goats. Data concerning the time frame, the device type, the error type, total matches, and average score appear at the top of the display. The center of the display is a graph of the probability of error at selected threshold values represented as ranges. Under the graph is a tabular representation of the data in the graph along with the precision and confidence for each probability. Six reports are generated each batch processing period covering both error types for all three devices. These reports represent the operation of individual PIV devices without the benefit of the hybrid.

Because the hybrid system recognizes the existence of goats and is designed to allow for their presence in any population, the report labeled "Operational Performance Curve," Figure A-28, is included to reflect the actual operation of the hybrid. During actual operation, the system routes goats around the device most likely to cause an error. This process is reflected by displaying the error probability curve with actual goat data removed. Additional information regarding goats is included in this report. The report lists the time frame represented, the device type, the error type, the total matches used to create the curve, the total quantity of goats excluded, the percentage of population as goats, the average score for all users, the average score of actual goats, and the average score for all users without goats. The center of the display contains the error probability graph generated from all scores less goats. The bottom displays tabular data with the confidence and precision.

By comparing the true curve to the operational curve, a measure of hybrid effectiveness is obtained. Six operational reports are generated each period to coincide with the six true reports. It is expected that these reports will be printed and

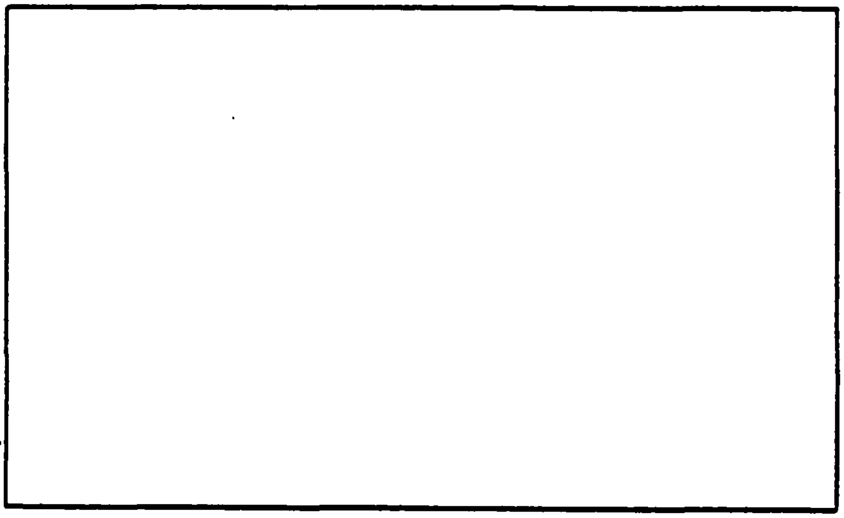
```
TRUE PERFORMANCE CURVE FOR TIME FRAME  (date)  TO  (date)
DEVICE  ------------------          TOTAL MATCHES  --------
ERROR TYPE  --------------          AVERAGE SCORE  --------


ERR
PROB
(%)



RANGE      1     2     3     4     5     6     7     8     9     10
PROB     .xx   .xx   .xx   .xx   .xx   .xx   .xx   .xx   .xx   .xx
PREC    x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx
CONF (%)  xx    xx    xx    xx    xx    xx    xx    xx    xx    xx
```

HEADING	DESCRIPTION
DEVICE	The device type.
TOTAL MATCHES	Quantity of matches.
ERROR TYPE	Type I or Type II.
AVG SCORE	Average score value.
RANGE	Ten class intervals.
PROB	The error probability for that class.
PREC	The precision of the error probability.
CONF	The confidence in the error probability.

Figure A-27: TRUE ERROR PERFORMANCE REPORT

```
OPERATIONAL PERFORMANCE CURVE FOR TIME FRAME  (date)  TO  (date)
DEVICE  ________________       TOTAL MATCHES  _________
ERROR TYPE  _______   TOTAL GOATS  _____ %POP AS GOATS  _______
AVG POP SCORE____  AVG GOAT SCORE_____  AVG SCORE NO GOATS_____
```

ERR
PROB
(%)



```
RANGE       1     2     3     4     5     6     7     8     9    10
PROB      .xx   .xx   .xx   .xx   .xx   .xx   .xx   .xx   .xx   .xx
PREC     x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx  x.xx
CONF (%)   xx    xx    xx    xx    xx    xx    xx    xx    xx    xx
```

HEADING	DESCRIPTION
DEVICE	The device type.
TOTAL MATCHES	Quantity of matches.
ERROR TYPE	Type I or Type II.
TOTAL GOATS	Quantity of goats.
%POP GOATS	Percent actual goats.
AVG POP SCORE	Average score all users.
AVG GOAT SCR	Average score all actual goats.
AVG SCR NO GOATS	Average score of all users less actual goats.

Figure A-28: OPERATIONAL ERROR PERFORMANCE REPORT

saved for use in future device acquisition, as well as to provide some insight into possible device degradation.

12. SCORE DISTRIBUTION CURVES

The report entitled "Score Distribution Curve," Figure A-29, is actually a preliminary step in the generation of performance curves. During each batch processing period, twelve distribution curves are generated. Four curves for each device represent score distributions for Type I error analysis of scores with goats and without goats, and for Type II analysis of both goat designations. The upper part of the display shows the time frame covered, the curve type (operational or true), the device, the total scores used in the curve, the error type, the total goats either used or excluded, the percentage of population being goats, the average score for this curve, the mean for this curve, and the standard deviation of this curve. The center of the display is a graphic representation of score distribution. It is an equal class interval distribution with a class interval of ten. A tabular display of the number of occurrences in each class is included under the graph. Information used to generate these reports result from the batch process and is contained in files especially created for this purpose. Score distribution curves will be printed and saved along with the error performance curves.

D. ON DEMAND REPORTS

Reports having no particular time constraints are included in the on demand group. These reports, which are available at any time, include data on visitors, personnel, alarms, and inventory. They have been designed for general use and can be requested through function keys.

```
SCORE DISTRIBUTION CURVE FOR TIME FRAME  (date)  TO  (date)
CURVE TYPE __________  DEVICE  _________  TOT SCORES  _____
ERROR TYPE ______ TOT GOATS ______ %POP AS GOATS _____
AVG SCORE _______ MEAN  __________ ST DEV  ________

#HITS

RANGE       1    2    3    4    5    6    7    8    9    10
OCCUR      xxx  xxx  xxx  xxx  xxx  xxx  xxx  xxx  xxx  xxx
```

HEADING	DESCRIPTION
CURVE TYPE	Either operational or true.
DEVICE	The device type.
TOT SCORES	Quantity of scores used to generate the curve.
ERROR TYPE	Type I or Type II.
TOT GOATS	Quantity of goats, this device, this error.
%POP GOATS	Goats as a percent of the population.
OCCUR	The quantity of scores falling within the range (= #HITS).

Figure A-29: SCORE DISTRIBUTION CURVE REPORT

1. TRANSACTION TRACE REPORT

One of the most valuable reports, in terms of security, is labeled "Transaction Trace," Figure A-30. This report is an audit of entry activity specified by user or time frame. If no user is specified on the report, the software searches the transaction record and lists all entry activity for all users within the time frame requested. This built-in capability allows an examination of a single entry attempt or any number of entry attempts at any point in time. The included data consists of the user's ID, which is input by the operator, and the time frame to be searched, which is also input by the operator. The user's name and social security number may be used as an alternate basis for the search but is automatically listed if only the ID number is input. The transaction record is then searched, creating a temporary working file containing the total quantity of attempts occurring in the time frame along with the quantity of rejections. The Type I error rate is figured and listed along with the confidence and precision. The report then lists each entry attempt made by the specified user during the specified time frame. Included in this list is the date and time of each attempt, the portal ID, the OOD in effect, the thresholds and match scores from each device in the portal, the throughput time for the attempt, any alarms occurring in the portal during the attempt, and the final accept/reject decision generated by the HIU. All entry attempts made by the specified user within the specified time frame will be listed.

2. VISITOR REPORT

The visitor report, Figure A-31, is a more detailed examination of visitors obtained from data kept in the visitors history file which is created as the visitor schedule. This report deals with all aspects of the visitor relevant to the

TRANSACTION TRACE

USER ID: ----------------------------

NAME: ------------------------------

SSN: -------------------------------

TIME FRAME: -------- THRU --------

TOT ATTEMPTS ---- TOT REJ ---- %ERROR ---- PREC ---- CONF ----

DATE-TIME	PORT	OOD	1TD	1MS	2TD	2MS	3TD	3MS	TPUT	ALM	SYSA/R
xxxxxxxx	xx	xx	xx	xx	xx	xx	xx	xx	xxx	xx	x

(ALL ENTRY ATTEMPTS WITHIN THE TIME FRAME WILL BE LISTED)

HEADING	DESCRIPTION
TOT ATTEMPTS	The quantity of attempts this user.
TOT REJ	The quantity of rejections.
%ERROR	Type I error rate.
PREC	Precision of error rate.
CONF	Confidence in error rate.
DATE-TIME	Date and time of each attempt.
PORT	Portal ID of attempt.
OOD	The OOD in effect.
nTD	Threshold setting, device n.
nMS	Match score, device n.
TPUT	The total portal time.
ALM	The alarm, if any.
SYSA/R	The final system accept/reject decision.

Figure A-30: TRANSACTION TRACE REPORT

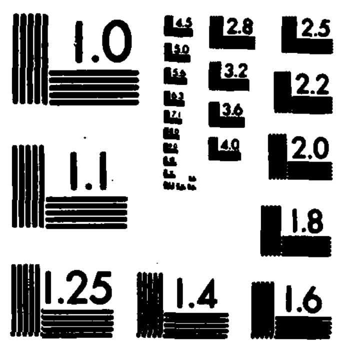
AD-A147 922 HYBRID TECHNIQUES INVESTIGATION(U) SHANE-GELLING CO SEA CLIFF NY D C SHANE ET AL. APR 84 SGR-84-01 RADC-TR-84-60 F30602-82-C-0167 3/3

UNCLASSIFIED F/G 17/2 NL

END

FILMED

DTIC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0

VISITORS REPORT

NAME:

SSN:

VID:

SLC:

COMPANY AFFILIATION:

DATE OF VISIT:

TIME OF VISIT:

PERSON VISITED:

REASON FOR VISIT:

VIS CARD ISSUED:

ISSUED BY:

TIME ISSUED:

PLACE ISSUED:

ACCESSIBLE AREAS:

AUTHORIZED TIME FRAME:

AUTHORIZING OFFICIAL:

DESIGNATED ESCORT:

NEED TO KNOW: (DD-254 IF MILITARY)

TIME VISITOR LEFT:

Figure A-31: VISITORS REPORT

secure facility. Records on visitors are kept in disk memory and the report is available through the function keys.

3. PERSONNEL REPORT

The personnel report, Figure A-32, is an image of each user's personnel file kept separate from all other personnel files on the facility. This file contains data useful to security personnel and is used to locate individuals within the facility among other things. Included in this report are the user's name, ID, social security number, job title, job classification, job area, job phone, security level clearance, the areas accessible to the user, the user's authorized entry time frame, authorized entry points, and the user's physical characteristics. This report may be specified by name, ID, or social security number and is accessible through function keys.

4. ALARM FILE REPORT

The alarm file report, Figure A-33, is a display of the contents of the alarm file specified by alarm condition. This file is used by the alarm response software and contains data used to support the alarm screen. It lists the alarm, priority, suppression times, the map number, planned response personnel and times, along with the planned response in both code and English text. This file may be accessed and viewed through the alarm file report. Other alarm handling software allows changes in this file. No changes can be made to the file contents through this report.

PERSONNEL REPORT DATE ---------- TIME --------

NAME:

ID:

SSN:

JOB TITLE:

CLASSIFICATION:

JOB AREA:

PHONE:

SECURITY LEVEL CLEARANCE:

ACCESIBLE AREAS:

AUTHORIZED TIME FRAME:

AUTHORIZED ENTRY POINTS:

PHYSICAL CHARACTERISTICS:

Figure A-32: PERSONNEL REPORT

ALARM FILE REPORT DATE ---------- TIME --------

ALARM CONDITION:

PRIORITY:

SUPRESSION TIMES:

MAP NUMBER(s):

PLANNED RESPONSE PERSONNEL:

PLANNED RESPONSE TIME:

PLANNED RESPONSE (CODE):

PLANNED RESPONSE (TEXT):

Figure A-33: ALARM FILE REPORT

5. INVENTORY CONTROL

Inventory control, Figure A-34, is a report designed specifically for maintenance personnel. It is used to keep track of spare parts used in the hybrid system. It identifies the parts by number and an English description. It provides for ease of locating parts with the crib ID and storage locations. Also listed are the quantity on hand, the order point, the quantity on back order, and a listing of how each part has been used during the previous year. Primary part suppliers are listed along with secondary sources of supply. A similar part entry guides maintenance personnel to alternate parts in the event there are no parts available with the specified number. The similar use entry lists other facilities utilizing this part number. This report provides data on part cost as well as availability, which is valuable in forecasting budget requirements. The inventory file is kept current by clerical personnel who update the file every time a part is required. A copy of the part number, description, and storage locations is given to maintenance technicians on demand to make servicing the hybrid system as easy as possible.

ECS INVENTORY CONTROL DATE ----------

PART NUMBER --------------- UNIT COST ----------

DESCRIPTION ---

CRIB ----------- STORAGE LOCATION -----------------

QUANTITY ON HAND ---------- QUAN ON B/O ----------

ORDER POINT --

PREVIOUS USE:

1 -------- 2 -------- 3 -------- 4 --------

5 -------- 6 -------- 7 -------- 8 --------

9 -------- 10 -------- 11 -------- 12 --------

TOTAL ------------------

PRIMARY SUPPLIER ------------------------------------

SECONDARY SUPPLIER ------------------------------------

SIMILAR PARTS ---------------------------------------

SIMILAR USE ---------------------------------------

Figure A-34: INVENTORY CONTROL REPORT

GLOSSARY

ASV	- Actual Score Value resulting from a match attempt in a PIV.
C3P	- Command, Control, Communications Processor.
DMA	- Direct Memory Access.
ECP	- Entry Control Point.
ECS	- Entry Control System.
GOAT	- An enrolled person who obtains consistently bad scores on a PIV.
HIU	- Hybrid Interface Unit; integrates PIV's, Host; controls portal
HYBRID	- A System of Multiple PIV's whose errors are commandable at Base level
IDENT	- ID File Processor.
ICP	- Individual Channel Processor; downloads and buffers the Host for timing purposes.
KBAUD	- Kilobytes per second.
LCT	- Logical Configuration Table; system Alpha, Beta, under each of the logical combinations.
OOD	- Order-of-the-Day; a table of computed PIV thresholds defining the desired system security.
OPC	- Operational Performance Curve; a measure of Alpha,Beta on any PIV excluding goats.
PIN	- Personal Identification Number.
PIV	- Personal Identity Verifier.
PROFICIENCY RATING	- A number in the authorization table in the portal indicating the entrant's PIV proficiency.
RAW DATA	- Entrant's entire feature set, this entry.
RFF	- Reference Feature File.
RFP	- Reference File Package.
SBMP	- Single Board Microprocessor.
SDC	- Score Distribution Curve.
THRESHOLD	- Decision Score Level.
TPC	- True Performance Curve; a measure of Alpha,Beta on any PIV including goats.

BIBLIOGRAPHY

1. Birnbaum, A., Confidence Curves: An Omnibus Technique for Estimation and Testing Statistical Hypotheses, Journal of the American Statistical Association, Vol. 56, No. 294, June 1961.
2. Doddington, G.R., Speaker Verification, RADC-TR-74-179, April 1974.
3. Fejfar, A., Test Results Advanced Development Models of BISS Identity Verificaion Equipment, Volume I, Executive Summary, ESD-TR-78-150, Vol. I, July 1978.
4. Foodman, M.J., Test Results Advanced Development Models of BISS Identity Verification Equipment, Volume II, Automatic Speaker Verification, ESD-TR-78-150, July 1978.
5. General System Specification for the DOD Base and Installation Security System (BISS), BIS-SYS-10000A, April 1982.
6. Grant, E.L., Statistical Quality Control, (2nd Edition), McGraw-Hill, N.Y., 1952.
7. Harold Rosenbaum Associates, Entry Control System Analysis: Hybrid Control Study, RADC-TR-82-28, Vol. 1, March 1982.
8. Hays, William L. and Robert L. Winkler, Statistics: Probability, Influence and Decision, Holt, Rinehart and Winston, Inc., New York, 1971.
9. Kendall, M.G., and W.R. Buckland, A Dictionary of Statistical Terms, Oliver and Boyd, London, 1957.
10. Owen, D.B., Table of Factors for One-Sided Tolerance Limits for a Normal Distribution, Sandia Corporation Monograph SCR-13, April 1958.
11. SRI International, Automatic Palmprint Verification, F30602-79-C-0207, January 1981.
12. Texas Instruments, Voice Verification Upgrade, RADC-TR-82-139, June 1982.
13. U.S. Department of Commerce, Experimental Statistics, M.G. Natrella, National Bureau of Standards Handbook 91, August 1963.
14. U.S. Department of Commerce, Guidelines on Evaluation Techniques for Automated Personal Identifiction, National Bureau of Standards, Federal Information Processing Standards Publication 48, April 1981.

MISSION
of
Rome Air Development Center

RADC plans and executes research, development, test and selected acquisition programs in support of Command, Control Communications and Intelligence (C^3I) activities. Technical and engineering support within areas of technical competence is provided to ESD Program Offices (POs) and other ESD elements. The principal technical mission areas are communications, electromagnetic guidance and control, surveillance of ground and aerospace objects, intelligence data collection and handling, information system technology, ionospheric propagation, solid state sciences, microwave physics and electronic reliability, maintainability and compatibility.

END

FILMED

12-84

DTIC